Defense Information Systems Agency
A Combat Support Agency

Defense Information Systems Agency

Terms and Conditions

Applicable to All Service Level Agreements

Published Date:
November 2015

Version 5.0.1

Revision History

Date	Version Number	Section Reference	Changed By	Description
12/2009	3.0	All	CD27	Updates to all sections
4/2012	4.0	All	CD27	Format changes and content updates throughout.
6/2012	4.1	Sect 6; Appendices G,H	ES24	Updated Sect 6 to reflect the current 10 USC Section 2222 requirements; updated the 10 USC links in App G-References; added App H – Performance Standards.
9/2012	4.2	Sect 5,10; Appendices E,F,I	ES24	Sect 5 – Updated FMLO email Sect 10 – Added note that DEE CMI min charge has changed to $2.5K Added the following acronyms to the acronym and/or glossary lists: ATC, CAP, CCC, CP, ECA, IATO, IECA, IPC, LECA, LIECA, OOB Added Appendix H (previously I) – GCDS Performance Stds / Responsibilities
5/2013	4.3	Sect 1-7,10; Appendices A-C,E	ES244	Added info re: socializing changes to the Agreement with the partner; moved IOE, IOC, and FOC definitions from 5.0 to 2.0 (first instance of usage); clarified timing guidance for completing the draft/final SLA; added FISMA reporting info; updated IRB website URL; added statement re: Partner PM IA duties; other standard changes
7/2013	4.4	Sect 2; Appendices B,I	ES244	Added note to Sect 2 re: Partner Program & Financial Mgrs; added Vendor POC row to SW Transfer form; updated GCDS Perf Stds
10/2013	4.5	Sect 8-10; Appendices C,G	ES244, ES535	Added verbiage re: A-goal & C-goal pricing in Sect 2; added communications input in sect 8; revised references to IA Architecture and updated them to DoD DMZ Extension; changed verbiage re: partner-owned HW in Sect 9; revised DMZ verbiage & added VMS link in sect 10; corrected Combatant Command acronym in App C; updated references in App G

Date	Version Number	Section Reference	Changed By	Description
3/2014	4.6	Sect 1,9,10; Appendices A,B; All	ES454	Removed statement re: DoDI 4000.19 in Sect1, #1 and Sect.7, #2; added verbiage re: partner-owned HW to Sect 9 (para 4-7); updated information re: classified info spillages in Sect 10 (#9); added Termination Worksheet and SW Transfer Agreement forms as attachments to this doc; changed Enterprise Services Directorate/ESD to Enterprise Information Services/EIS
4/2014	4.6.1	Sect 4,5,7,10; Appendices E,G,H	ES454	Changed IOE to IOC for SLA creation; corrected FMLO email; replaced FRS with DCAS; added note that SIPRNet link won't work unless on SIPRNet; updated links in References; corrected SyNAPS link
6/2014	4.7	Sect 2,8	ES454	Added Sect 2, Onboarding Paths; added clarifying verbiage to Sect 8, Duration and Termination of Agreement
12/2014	4.8	All	ES454/SI81	Changed EIS to DISA, font from TNR to Arial; removed Appendix D – Inherited IA Controls and added all IA Control documents as attachments; added milCloud and milCloud Plus info to Sects 2, 3, 6, & 11; added info on C&A expiration process to Sect 4, reqd MIPR details to Sect 6, new guidelines on partner response times to annual reviews and re-signatures of new / existing SLAs to Sect 8, verbiage to that addresses partner application SW to Sect 8, security updates to Sect 11, audit request info to Sect 12; updated server HW in Sect 10; updated References and Perf Stds appendices

Date	Version Number	Section Reference	Changed By	Description
10/2015	5.0	All	BDM52	Changed the cover, header, and p1 from DISA EIS T&C to DISA T&C based on DISA reorg; additional verbiage/clarification on change requests (Sect4, #7); additional verbiage/clarification on workload history for estimate creation (Sect4,#11); additional HW/OS listed and z/Linux info (Sect9,#2,a); added ex of comm networks (Sect9,#2,c); added CoN info and reference (Sect11,#1,c & App F); spelled out all instances of IS (information system); updated JTF-GNO to USCYBERCOM; made grammatical corrections throughout; removed references to SyNAPS; changed the terms Classified Information Spillage (CIS) and Classified Messaging Incident (CMI) to Negligent Discharge of Classified Information (NDCI) per SecDef memo; changed “CME” to “Engagement Executive throughout; updated GCDS Perf Stds/Responsibilities (App H); added note for clarity to Sect6,#2,b; updated CNDSP (App C); updated acronyms & references; added Audit info (App I); updated IA control docs; added verbiage re: CALs; replaced VMS w/ CMRS
11/2015	5.0.1	Appendix C	BDM52	Added 2 clarifying paragraphs and COLS-NA acronym to the beginning of the CND appendix

Table of Contents

1.0 Introduction

The Terms and Conditions (T&C) constitutes the policies of the Defense Information Systems Agency (DISA) overarching Agreement with all Department of Defense (DoD) Service and Agency partners for whom these Centers provide Computing and Enterprise services. As multiple directorates within DISA perform the roles and responsibilities involved in providing these services to the partners, the parties involved will hereinafter be referred to as "DISA" and "partner." The Agreement is made up of the following:

1) Service Level Agreement (SLA) – documents the service(s) DISA is providing to the partner. All services provided by DISA shall be documented in an SLA. Stated service levels shall be achieved by the resources allocated to satisfy the partner's projected workload and scheduled priorities. These service levels may be affected if there is a significant workload change or if the partner changes scheduled priorities without advance notice to DISA.
2) Planning Estimate (PE) – estimates the cost for sustainment of services provided to the partner each fiscal year (FY), from the first of October through the 30th of September. The PE is created by DISA for the partner as a planning and budgeting tool for the services DISA provides.
3) Service Catalog – provides descriptions of each service DISA offers, as well as services being developed in the pipeline. DISA shall only provide those services advertised within the Service Catalog, and unless otherwise specified in the SLA, these services shall be delivered as described in the Service Catalog.
4) T&C – constitutes the policies of DISA's Agreement

Specific services, rates, and costs are outlined in the Agreement. There are links from the SLA to both the Service Catalog and T&C. The content of the Service Catalog and T&C is also considered to be content of the SLA. The information in the Service Catalog and T&C shall not be restated in the SLA.

A Letter Estimate (LE) establishes the basis for, or changes to, the SLA. It is submitted to the partner as a result of a request for new, or changes to existing, workload. The LE restates the partner expectations/mission, requirements, assumptions, and the recommended technical solution. It also includes the estimated cost for implementation and sustainment of the new or changed workload.

Any change to the SLA, Service Catalog, or T&C that impacts the overall Agreement will be socialized with the partner by their respective Mission Partner Engagement Executive Team.

The T&C is effective upon partner signature of the LE.

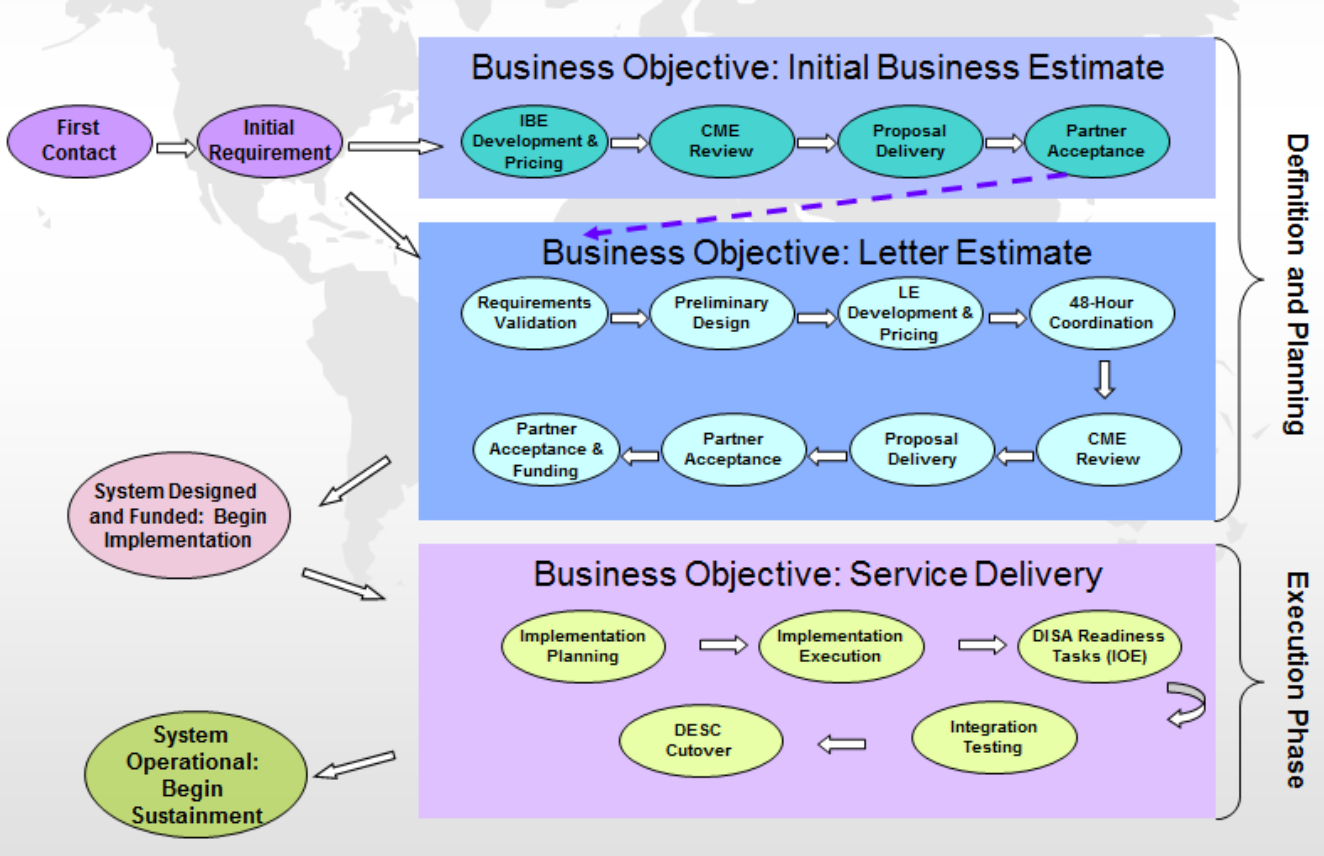
2.0 Onboarding Paths

1) milCloud Infrastructure as a Service (IaaS) Self-Service
   a) Provides real-time, self-service cost and provisioning of virtual workload via the Cloud Services Marketplace Portal at: https://milcloud.mil.
   b) All milCloud workload is partner-managed under the authority of the partner's Designated Approving Authority (DAA)/Authorizing Official (AO).
   c) Partners will be given direct network access to the DISN for their provisioned workload after coordinating DAA/AO acceptance of responsibility with DISA.

The full terms and conditions for self-service Virtual Data Centers (VDCs) can be found by accessing the Cloud Services Marketplace at https://milcloud.mil and clicking on Order > VDC in the upper left-hand corner of the home page.

2) End-to-End (E2E) – The E2E fulfillment process governs the project workflow for new partner Computing and Enterprise Service workloads hosted by DISA and any changes to those workloads. The E2E process outlines the initiation, definition, planning, and execution of the technical projects that result from these hosted services.
   a) Streamline Standard
      i) Streamlined engineering (only operating systems [OSs] supported by capacity services contracts and standard network architecture apply)
      ii) Provisioning timelines vary per OS type specified
      iii) No partner-provided network devices allowed
   b) E2E Non-Standard (Custom)
      i) Complex engineering effort (may contain non-standard architecture)
      ii) Provisioning timelines vary per solution design specified
   c) milCloud Plus (DISA Engineered/Managed)
      i) Baseline/build documentation engineered by DISA
      ii) Implementation by DISA
      iii) Provisioned by DECC on behalf of the partner
      iv) DISA-managed VDC
      v) milCloud optional services (i.e. system and database administration)

3.0 Business Estimate Process



1) milCloud IaaS Self-Service – Provides cost estimates and real-time provisioning of all workload through the Cloud Services Management portal available at: https://milCloud.mil.

2) Initial Business Estimates (IBEs) and LEs – While both IBEs and LEs rely on partner requirements, IBEs do not require a significant level of detail to produce a price estimate, and typically will not have a full technical solution. LEs, on the other hand, are fully developed proposals that address complete partner requirements. An IBE is an option for the partner and may be bypassed altogether in favor of an LE. Target completion timeline for an IBE is 10 working days following the agreement of requirements. The LE is the starting point for new workload, or additions to existing workload, and therefore demands a greater amount of information, technical analysis, pricing and overall development of the document. Target completion timeline for an LE is approximately 30 business days following the agreement of baseline requirements.

3) Process Steps

   a) IBE

      i. First Contact – Initial communication between the partner and DISA. Outcomes include a tracking system entry, tracking number assignment, team/lead assignment, and delivery of service documentation (Service Catalog and T&C) and forms (Service Request Form [SRF]) to the partner.

ii. Initial Requirement – The DISA Customer Relationship Management Branch team lead works with the partner to attain high-level system hosting requirements. Outcomes include a tracking system update, completed (high-level) SRF for IBE development and pricing, and determination (with the Engagement Executive) of ability to respond.

iii. IBE Development and Pricing – As described above, the IBE is a method of delivering a quick price estimate to the partner. The development of the document should restate high-level requirements, and the pricing should reflect general values related to A-goal (OSD-approved partner billing rate) and C-goal (reimbursable cost of services) service prices. Outcomes include an IBE, pricing entry, and a tracking system update.

iv. Engagement Executive or Division Review – All IBEs shall be reviewed at the Engagement Executive-level or above prior to delivery to the partner. At the division chief's discretion, the 48-hour Coordination (two business days) step may be utilized. Outcomes include an approval or non-approval for delivery along with a tracking system update.

v. Partner Delivery – Formal delivery shall consist of an e-mail or other approved correspondence vehicle that shall allow for a date, time and designated partner to track progress. Outcomes include delivery to the partner and a tracking system update.

vi. Partner Acceptance – The partner who chooses to accept or move forward from the IBE shall be informed that an LE will now be developed, which involves detailed requirements, a technical solution, implementation planning, and a more explicit price estimate.

b) LE

i. First Contact – Initial communication between the partner and DISA (if the IBE path was not followed). Outcomes include a tracking system entry, tracking number assignment, project lead assignment, and delivery of the SRF to the partner.

ii. Project Team – The DISA project lead and Information Assurance (IA) Technical Advisor work with the partner to attain in-depth system hosting requirements and address numerous issues. These issues include the partner's IA posture; network/communication considerations including the registration of ports (internal and external); the partner's integrated milestone schedule; and funding and resource availability. Outcomes include a tracking system update, completed SRF, creation of a solution document for LE development and pricing, Bill of Materials (BOM) initiation, IA risk assessment, and determination (with Engagement Executive) of DISA's ability to respond.

iii. Solution Document – DISA team (including appropriate engineering, capacity, operations, communications, IA, and other necessary representatives) develops a general plan for the implementation and management of the partner workload. Outcomes include a solution document, assumptions related to the solution, and a tracking system update.

iv. LE Development and Pricing – The development of the document shall restate partner expectations/mission, detailed requirements, assumptions, and the solution

summary. The pricing shall reflect the A-goal and C-goal prices for identified services. Outcomes include an LE and a tracking system update.

v. 48-Hour Coordination for Non-Standard Projects – To ensure that a formal proposal from DISA represents an accurate description and pricing of DISA services, coordination with DISA service and financial management teams is mandatory.

vi. Engagement Executive or Division Review – All LEs shall be reviewed at the Engagement Executive level or above prior to delivery to the partner. Outcomes include an approval or non-approval for delivery along with a tracking system update.

vii. Partner Delivery – Formal delivery shall consist of an e-mail or other approved correspondence vehicle that shall allow for a date, time and designated partner to track progress. Outcomes include delivery to the partner and a tracking system update.

viii. Partner Acceptance – The partner wishing to accept the LE shall be informed that DISA requires a formal approval, e.g., the signed LE, and initial funding to include the implementation (one-time charges) and initial three months' operating (recurring) funding.

c) Service Delivery – Upon partner acceptance and funding of an LE, DISA shall begin implementation planning and execution to implement the partner's project through Initial Operating Environment (IOE), Initial Operational Capability (IOC), and Full Operational Capability (FOC).

i. IOE – A system reaches IOE when accepted proposals/LEs have IT assets that have progressed successfully through implementation and have been turned over to the partner to load their application(s) and data.

ii. IOC – A system reaches IOC when the application has been loaded, tested, and opened to the user base for production.

iii. FOC – A system is declared FOC when it has been migrated into DISA service and has executed its function for the agreed-to period (30 calendar days after IOC declaration) without critical or high incidents, and it has completed all other defined exit criteria.

NOTE: The Partner's Program Manager approving project SRFs and the Partner's Financial Manager authorizing the obligation of funds must be government employees.

4.0 Management Process Responsibilities

1) DISA and the partner shall furnish all notifications and information to one another in writing via memorandum or electronic mail and by telephone, if urgent.
2) The partner shall work with the appropriate DISA representative to prioritize the partner's applications and to develop the Business Continuity Plan (BCP).
3) DISA shall meet with partner representative(s) to discuss performance; issues; areas of concern; anticipated workload changes; and any changes or modifications to the Agreement, BCP, or Risk Assessment and/or security posture.
4) To successfully integrate an application into the Continuity of Operations (COOP)/Service Continuity program, there are certain responsibilities which cannot be performed by DISA. The partner must:
   a) Possess a valid accreditation or authorization (using the DoD Information Assurance Certification and Accreditation Process [DIACAP] or Risk Management Framework [RMF]).
   b) Initiating requests for COOP capability exercises through the assigned Customer Account Representative (CAR). (Exercises are not conducted unless there is a partner request and partner involvement in the verification and validation of the recovery exercise effort.)
   c) Initiating termination or removal of COOP coverage for server-based processing.
5) Exercises of COOP capability require an initiating request from the partner through their assigned CAR.

   Any partner who has not contracted with DISA for COOP/Service Continuity services is specifically excluded from the DISA COOP/Service Continuity program and exercises. No promise or expectation of COOP/Service Continuity is implied or should be inferred. The SLA shall include an annotation that the partner has "No DISA-provided COOP" requirements that are to be satisfied by DISA.
6) DISA CARs shall notify the partner within 180 calendar days of an expiring Certification and Accreditation (C&A) or Assessment and Authorization (A&A) date. DISA must maintain situational awareness of partner accreditation decisions due to the impact and effect on DISA's risk boundary. The partner shall inform DISA of their expiration status. Subsequent follow up with the partner point of contact (POC) will occur every 30 calendar days after the initial contact. On the 120th calendar day, the notifications will pass over to the DISA Cyber Services Division. The Cyber Services Mission Partner Integration Team will engage with the partner program manager and Mission Partner Integration (MPI) personnel until the updated accreditation decisions/authorization and new expiration dates are provided.
7) The partner shall provide full, detailed documentation for any change requests recommended by DISA to improve the performance or security position of the customer workload the partner non-concurs with, providing specific information regarding the problem(s) the change request would introduce and/or specific reasons why the change request cannot be implemented at the time with which it is non-concurred.

8) When available, DISA Enterprise Services (i.e., DoD Enterprise E-mail [DEE] and DoD Enterprise Portal Service [DEPS]) shall be used in lieu of partner-unique application solutions.

9) DISA shall furnish to the partner a primary and alternate DISA POC, documented in the SLA, and update these as necessary.

10) The project lead shall furnish both the primary and alternate partner POCs to the appropriate DISA Service Desk via the Service Desk Requirements Form, and update as necessary. In the event the Service Desk cannot contact the primary POC, the alternate on the list shall be contacted. The partner POC shall notify the partner users of any operational situations that impact service.

11) The partner shall provide estimates of anticipated workloads with which DISA can develop a target budget amount for the PE. To aid in this estimate, DISA shall provide workload history from DISA's billing system (currently the Centralized Invoice System [CIS]), where it is available.

   a) Workload Estimates
      i. DISA shall provide the partner with actual mainframe and storage usage information, as well as server and server storage usage analysis being provided during the year. To develop meaningful projections, the partner and DISA should collaborate, as the partner is ultimately responsible for all mainframe and server projections.
      ii. The partner shall notify DISA of in-cycle changes to workload estimates or support requirements as they become known.
      iii. The partner shall furnish DISA with projections of future workload levels and support requirements at the Customer Identification Code (CIC) and the Application System Code (ASC) levels. These should reflect known or anticipated changes not less than 180 calendar days prior to the known change.
      iv. DISA shall respond to any in-cycle changes to workload estimates or support requirements after formal notification of such changes by the partner.

   b) Budget Estimates
      i. The partner uses workload estimate information to submit a budget estimate for funding.
      ii. If a difference between the partner budget submission and final approved appropriation exists, DISA, in conjunction with the partner, shall adjust the services in the SLA accordingly, matching services to the partner funding level.

   c) SLA Preparation
      i. The SLA shall be specific as to the types and levels of services required.
      ii. The partner shall furnish the projected workload for DISA to effect the proper level of support.
      iii. The SLA shall contain any additional DISA and/or partner responsibilities that are consistent with the workload rights and support.

5.0 Pricing

The PE is created by DISA for the partner as a planning and budgeting tool for the services DISA provides. The PE serves the following purposes:

1) Sustainment of Existing Workload – DISA shall provide the partner with a proposed PE no later than the third quarter of the current FY for the following FY. The PE is reviewed by the partner and DISA to confirm that it provides an accurate representation of support provided to the partner. The Partner shall ensure DISA receives a Military Interdepartmental Purchase Request (MIPR) for at least the first quarter of support, as invoiced in CIS, by the first of October of the following FY, or immediately upon passage of a Continuing Resolution or DoD Appropriations Act.
2) New Workload or Changes to Existing Workload – Upon signature of an LE, the DISA CAR shall begin creating an SLA for new workload or modifying an existing SLA. Within 30 calendar days after IOC is reached, the SLA must be drafted (new SLA) or modified (existing SLA) and provided to the partner for review. No later than FOC, the SLA must be bilaterally agreed upon and signed by the partner and applicable DISA representatives. If this modification requires additional funds for sustainment throughout the remainder of the current FY, DISA shall update the existing PE to reflect the change in cost. The Partner must submit funding for implementation costs prior to DISA beginning any implementation of the workload and the Partner is also obligated to provide a MIPR for the amount of the first quarter's increased sustainment.
3) New DISA Partner – Upon signature of an LE, the partner must submit funding for implementation costs prior to DISA beginning implementation of the workload. The MIPR shall provide funding to cover estimated charges for at least one quarter, with amendments executed prior to the start of each succeeding quarter.

6.0 Funding and Billing

1) Funding – Upon signature of the LE, the partner becomes obligated to pay DISA for the services identified in the LE.

   At the beginning of the FY, funding may be provided contingent on passage of a Continuing Resolution or DoD Appropriations Act, whichever is applicable. The partner shall submit all MIPRs to the Financial Management Liaison Office (FMLO). The FMLO shall submit a MIPR Acceptance Form (DD Form 448-2) to the partner acknowledging acceptance of the funds received.

   Upon receipt of the MIPR, DISA becomes obligated to provide the services documented in the LE. Within 30 calendar days after IOC is reached, the SLA must be drafted (new SLA) or modified (existing SLA) and provided to the partner for review. No later than FOC, the SLA must be bilaterally agreed upon and signed by the partner and applicable DISA representatives.

   In addition to the dollar amount, the MIPR shall contain the following:

   - The LE number and funding source
   - The Treasury Account Symbol (TAS) for both trading partners (DISA and partner)
   - The Business Event Type Code (BETC) for both trading partners. DISA-issued MIPRs are “DISB” (disbursement) and received MIPRs are “COLL” (collection)
   - The effective date and duration of the Agreement, to include the expiration of the funding source
   - The method of payment
   - The Business Partner Network (BPN) number for both trading partners
   - The method and frequency of performance (revenue and expenses) reporting
   - If applicable, provisions for advance payments and method of liquidating such advances
   - The parties’ rights to modify, cancel, or terminate the Agreement
   - Accounting/finance office POC information. This includes name, location, telephone number, and e-mail address, as well as: Resource Management Office, Customer Service Office, and Contracting Officer (KO) or KO’s Technical Representative (COTR) POC information.
   - An alternative Dispute Resolution clause
   - The SLA number assigned by DISA
   - Where practicable, the application and/or ASC (Block 9)

   MIPRs must also include the following minimum information in the MIPR Description field (Field 9b):

   - Dollar amount – Implementation: $XXX.XX
   - Dollar amount - ¼ (3 months) Annualized Recurring: $XXX.XX
   - Name, email, and phone number of partner financial POC

- Purpose and description of services being procured
- Trading Partner Number: DoD Activity Address Code (DoDAAC)
- Project Tracking Number: XXXX
- Implementation Billing Account Number (BAN) Code: XXXXXX
- Recurring BAN Code: XXXXXX

If an Implementation MIPR is required, it must abide by the following Project Order guidelines in Field 9b:

- Project name, DEPS number, and an adequate description of the environment to be implemented.
- Must include the following statements in their entirety:
  - "This order is placed in accordance with the provisions of 41 U.S.C. 6307, as implemented by DoD regulation."
  - "This order is for an implementation; it is non-severable and serves a bona fide need during the fiscal year the funds are obligated."
- To account for any possible schedule slippage, please use 30 September YYYY for all work to be implemented by the end of the current FY; otherwise, please use applicable scheduled date.

Funding documents shall be issued and addressed to:
DISA Enterprise Services – CFEB41/FMLO
The mailing address can be found in the partner's SLA and/or LE. When possible, funding documents should be e-mailed to: disa.pensacola-fmlo.eis.mbx.pen-miprmail@mail.mil. MIPR acceptance forms shall be e-mailed to the MIPR originator/issuer.

2) Billing – Routine billing shall commence at the beginning of each FY to reflect services provided. The partner may view invoices online at https://dwfn.csd.disa.mil/CustomerInvoices/default.aspx in the DISA CIS. Current period and year-to-date invoice data shall be updated bi-monthly, reporting actual charges incurred.

   The partner shall work with DISA to ensure partner account codes such as CICs, BANs, Industrial Fund Accounting System (IFAS) Codes, Invoice Account Codes (IACs), and ASCs are accurately assigned to capture usage data and service charges at levels useful to the partner.

   Partners within the Defense Finance and Accounting System (DFAS) Cleveland Financial Network shall be billed via the Defense Cash Accountability System (DCAS). All other partners shall be billed via the Intra-Governmental Payment and Collection System (IPAC). The partner shall promptly review the invoice, and notify DISA of any disputed billings. Subsequent partner billings shall include any adjustments arising from disputed billings.

   If the bill payer changes, the funding responsibility for an existing workload remains with the originating bill payer until the FMLO receives written notification of the new bill payer, the effective date, and a MIPR from the new bill payer. DISA and the FMLO should

receive this data at least 30 business days prior to the effective date. DISA shall change the appropriate CIC upon receipt of the new information, and shall document this information in the partner's SLA.

Server and Storage –

a) The recurring rate-based billing of a new server or operating environment (OE) and the raw storage, for new partner workload, begins at the time a server or OE is handed over to the partner for logon. This typically occurs at IOE. IOE is defined as the point when DISA has completed the initial system implementation (e.g., hardware installation, storage allocation, OS load, and hardening, to include Security Technical Implementation Guides [STIGs], IA Vulnerability Management [IAVM], etc.). At IOE the system is turned over to the partner to load their application and test the system. One-time implementation costs are also billed to the partner at this point.

b) For OEs that have undergone a technical refresh, when the new hardware is declared IOE, DISA allows 30 calendar days for parallel processing before the old environment is turned off. It allows for both sets of hardware to run parallel, with only one set billing, while any technical issues regarding the transition are resolved. At the end of the 30-day period, if the partner is not ready to decommission the refreshed hardware; both sets of hardware and raw storage shall be billed.

   NOTE: The 30 day timeline is for rate-based standard workload only and cost reimbursable items will be handled on a case-by-case basis.

c) milCloud & milCloud Plus pro-rate services on a 30-day basis allowing the partner to terminate services after a minimum of one month of service. Both services allow partners to increase or decrease Central Processing Units (CPUs), memory and storage resources, but users are billed at the highest resource use in a 30-day period.

7.0 Business Management Modernization Program

A defense business system modernization is the acquisition or development of a new defense business system, or any significant modification or enhancement of existing defense business systems (other than necessary to maintain current services). The partner must provide the Business Management Modernization Program (BMMP) documentation required by United States Code (USC), Title 10, Section 2222 to the Office of the Secretary of Defense (OSD) Defense Business System Management Committee (DBSMC) (established by USC, Title 10, Section 186). The partner is responsible for submitting a copy of the DBSMC certification results or certification control number for the proposed business system to DISA prior to DISA obligating funding for services. Failure to present the appropriate documentation precludes DISA from taking further action or providing services until the time documentation is submitted.

Funds available to the DoD, whether appropriated or non-appropriated, may not be obligated for a defense business system program that will have a total cost in excess of $1,000,000 over the period of the current future-years defense program submitted to Congress under section 222 of USC Title 10 unless—

1) The appropriate pre-certification authority for the covered defense business system program has determined that—
   a) the defense business system program is in compliance with the enterprise architecture developed under subsection (c) and appropriate business process re-engineering efforts have been undertaken to ensure that—
      i) the business process supported by the defense business system program is or will be as streamlined and efficient as practicable; and
      ii) the need to tailor commercial-off-the-shelf systems to meet unique requirements or incorporate unique requirements or incorporate unique interfaces has been eliminated or reduced to the maximum extent practicable;
   b) the defense business system program is necessary to achieve a critical national security capability or address a critical requirement in an area such as safety or security; or
   c) the defense business system program is necessary to prevent a significant adverse effect on a project that is needed to achieve an essential capability, taking into consideration the alternative solutions for preventing such adverse effect;
2) the covered defense business system program has been reviewed and certified by the investment review board established under subsection (g); and
3) the certification of the investment review board under paragraph (2) has been approved by the Defense Business Systems Management Committee established by section 186 of this title.

Documentation for above must be provided as part of the partner's acceptance of any BMMP solution offered by DISA before implementation of the project can proceed.

Office of the Deputy Chief Management Officer Defense Business Council (DBC) and Investment Review Board (IRB): http://dcmo.defense.gov/Governance/DefenseBusinessCouncil.aspx.

8.0 Duration and Termination of Agreement

1) Duration – The SLA between DISA and the partner shall have an indefinite lifespan. It shall be reviewed annually at a minimum, ensuring DISA is furnishing all the negotiated IT services required by the partner. The annual review provides a forum for the partner to identify future workload requirements or other required changes which shall be recorded in the SLA and corresponding PE.

   The review timeframe recommendation is to perform annual reviews concurrently with PE issuance to partners and/or within 30 calendar days of a support change implementation. Partners have 30 days from contact with a CAR to respond to annual review requests – whether it is a request to review the SLA for needed changes or concur on any changes made by DISA. If no response is received from the partner within 30 calendar days of the CAR's request, the SLA will be fully accepted as written and annotated as such in the Annual Review table.

   For a new or existing SLA that requires new signatures, within 30 calendar days after IOC is reached, the SLA must be drafted (new SLA) or modified (existing SLA) and provided to the partner for review. The support and services represented and documented in the SLA are considered valid for 30 calendar days from the date of the last DISA representative's digital signature. If no correspondence or Partner signature(s) are received within that time, the SLA will be considered fully accepted as written and annotated as such. Any subsequent changes will require the negotiation and preparation of a new document and re-signature from all parties.

2) Termination – DISA requires written notice 180 calendar days in advance of the partner terminating any services provided. DISA shall discontinue service as soon as reasonably achievable, but billing may continue for up to six months for actual costs or services provided during the six months. Termination charges may be applied to the partner per the Financial Management Regulation, Volume 11B, chapter 11, paragraph 110102.

   a) With assistance of the DISA CAR, the partner shall provide a completed Agreement Termination Worksheet (Appendix A) if one of the following occurs:
      i. The partner is eliminating DISA support/entire SLA.
      ii. The partner is decommissioning an entire application/ASC.

   b) The Termination Worksheet is not needed, but the partner must still provide written notification (i.e. digitally signed e-mail) to DISA, if:
      i. The partner is discontinuing an existing optional service such as database administration or application support, but not all support for an application/system.
      ii. The partner wants to de-install existing hardware, but not an entire suite of hardware or application/system. In this case the partner will open a ticket with their supporting service desk and notify their CAR.
      iii. The partner wants to de-install or discontinue use of existing reimbursable application software; software can be found on reimbursable tab of the PE.

9.0 System Technology

1) System Architecture
   a) Server – The standard Server Enterprise Architecture (SEA) is a set of minimum requirements for a server to be placed in a DISA environment. These standards were developed by taking into account best practices, network requirements, storage requirements and overall general knowledge of the Defense Enterprise Computing Center (DECC) environment.
   b) Storage – The Storage Enterprise Architecture (StEA) is based upon the DoD Joint Technical Architectural (JTA) Framework Version 6.0. The DoD JTA Framework was developed in accordance with (IAW) the Global Accounting Office (GAO) Enterprise Architecture Management Maturity Framework and is maintained in the DoD Information Technology Standards Registry (DISR).
   c) Communications – The DMZ Extension architecture is designed around the DoD Network Security Technical Implementation Guide (STIG) (V7R1) which defines the requirement for physical separation between publically accessible web servers and other application server types. This architecture enables all applications to meet the task order mandated by CyberCom: CTO-12-371 as well as DoD Directive 8500.1, 4.12. These separate enclaves comprise the DECC. Architectures also exist which provide connectivity for management and replication of data for disaster recovery.
2) Configuration
   a) Server – There are four main hardware server platforms in DISA:
      - Itanium-based servers from HP
      - Power7-based servers and mainframe servers from IBM and Unisys
      - x86-based servers from HP
      - SPARC-based servers from Oracle

      The capacity services contracts provide hardware and OSs that include HP Windows, HP UNIX, Sun Solaris, IBM AIX, SUSE Linux, Red Hat Linux, zOS, zVM, and Linux on System z (z/Linux) (SUSE & Red Hat).

      DISA uses virtualization technology for server workload. In the Intel™ space this is accomplished with VMware Virtual Infrastructure. VMware has a myriad of capabilities such as VMotion (moving a running virtual machine [VM] from one physical server to another with zero downtime); Distributed Resource Scheduling (DRS), which is the capability to place up to 32 physical servers into a resource pool where workloads can utilize resources on the fly; and high availability (HA) which allows a VM to be started on another physical host automatically in the case of a hardware failure.

      In the UNIX space, virtualization and vendor partitioning methods are varied, but the following is a basic description: Physical or hard partitioning subdivides a single server, such that all power, CPUs, memory, and Input/Output (I/O) devices used by a partition are dedicated to that partition and no other. A physical partition has the following characteristics:

- Dedicated power. Power can be shut off to the partition without impacting any other partition.
- CPUs and memory are allocated to the partition based on hardware configuration and cannot be shared with another partition or be dynamically reallocated.
- All I/O devices are dedicated to the physical partition including Ethernet cards, Host Bus Adapter (HBAs), internal disk drives, and optical drives.
- May be configured as a single OS, or host multiple virtual OSs.

In the IBM z/Linux mainframe space, virtualization is accomplished with logical partitions (LPARs). LPARs are managed by an IBM processor resource/system manager (PR/SM) and can share I/O and CPUs, with dedicated memory to each LPAR. Each LPAR will host its own OS (zOS, zVM, z/Linux). zVM is also a virtualization environment that can act as a hypervisor for other OSs (zOS, zVM, z/Linux) running as separate OEs. zVM can virtualize hardware resources (CPU, I/O, memory) and can share with OEs within a given zVM. z/Linux OEs can host SUSE Linux and Red Hat Linux.

Virtual or soft partitions may have some attributes of physical partitioning, but not all, depending on the server and OS manufacturers. Generally, you may have multiple virtual partitions within a server, or within a physical partition. Resources (CPU, memory, and I/O) can be shared between the virtual partitions, either dynamically by the operator, or during boot-up configuration.

b) Storage – disk and tape technologies are the major data storage technologies used to support all OSs.
   - Disk is used to hold databases, data warehouses, and flat files where immediate access to the data is necessary.
   - Traditional and virtual tape is used for backups, archives, and for those files that do not need to be immediately accessed.

   The foundation of the architecture is a high-speed Storage Area Network (SAN) consisting of fibre channel (FC) switches connecting servers to their storage devices at each processing location. However, in special cases, with associated documentation, DISA can deploy Network Attached Storage (NAS) solutions. The SAN provides all standard storage functionality such as mirroring, data replication, data snapshots, data archiving, and security protection. The SAN supports all platforms at the processing location and can expand or shrink to meet changing requirements. Storage devices on the SAN are low cost and highly reliable. Boot-from-SAN is the standard architecture for all DISA-hosted platforms. Internal storage is only provided with server installations as a last resort when absolutely necessary. This architecture provides redundancy and highly available OS partitions and reduces outage times due to internal disk failures.

   DISA Enterprise Backup Network (EBN) employs a high speed Internet Protocol (IP) based network with automatic tape libraries to support the data backup and archiving process. DISA has an off-site tape storage contract for safe and efficient tape storage.

In the mainframe environment, storage devices are often shared physically and/or logically between processing platforms while the server environment primarily relies upon dedicated storage resources at the OS level.

c) Communications – The architecture is comprised of three standalone networks (Production, Out-of-Band [OOB]/EBN, DMZ Extension), each isolated from the others. Each network utilizes its own network space, virtual local area networks (vlans), and access control.

   i. Production – This network provides user level access to the application. Depending on the classification of the application and server it resides on, it will either sit in the web DMZ extension architecture or the production architecture. All traffic traverses a firewall inbound and outbound. The firewall also acts as the aggregation point for web and non-web traffic. Connections are also able to be load-balanced to provide reduced processing overhead and greater availability.

      A test and development (T&D) architecture also exists as a subset of the production network. This architecture provides separation from production applications as dictated by the STIG. Provisions for T&D Zone A-D are available.

   ii. Data Replication – This network is comprised of point-to-point circuits between DECC or Core Data Center (CDC)/Enterprise Operations Center (EOC) locations. It provides secure, IP based network transport for SAN, mainframe, tape and host-based replication.

   iii. OOB – This is the dedicated management network. It utilizes encrypted connections (Secure Socket Layer [SSL] and Internet Protocol Security [IPSec]) between the user and the hosting site to provide management capability for servers, applications and network devices. It also provides transport of monitoring and reporting devices.

10.0 Ownership and Licenses

1) Data – As the service provider, DISA is required to certify and accredit the platforms/systems or data operating in the DECCs. The partner operating applications on the systems within the DECCs is required to certify and accredit the applications as the owner of the data processed/produced in these applications and IAW the Federal Information Security Management Act (FISMA) and other regulations.

2) Hardware – DISA has negotiated a series of indefinite-delivery/indefinite-quantity capacity services contracts to obtain Unisys and IBM mainframes and IBM Power servers, Oracle SPARC servers, HP Itanium servers, and HP x86 servers.

   DISA is responsible for all equipment within the DECC. DISA manages, tracks, and maintains accountability for this equipment. These DISA responsibilities are covered by the basic services provided to the partner, and include establishing and maintaining auditable accountable records in the Defense Property Accountability System (DPAS), capitalizing and depreciating assets requiring capitalization, maintaining supporting documentation, hand receipting, and performing annual physical inventories and reconciliations.

   Maintenance Support – DISA requires a standard level of maintenance support for all assets owned and maintained by DISA. Maintenance support is based on DoDI 8500.2 MAC requirements. MAC I/II systems require 7/24/365 support, with a two (2) to four (4)-hour response time for maintenance and immediate response on parts. Maintenance support for MAC III systems is defined as next business day with same day parts arrival.

   Partner/Vendor-Owned Hardware Assets – DISA policy states that DISA shall no longer accept partner-owned equipment after the first of October, 2011. Partner-owned equipment currently residing in DECCs shall be grandfathered until end-of-life and technical refresh.

   Partners with approved, grandfathered hardware are obligated to provide complete lists of all assets, including communications hardware. Lists must include the following information for each asset:

   - Make
   - Model
   - Serial Number
   - Barcode
   - Physical Location
   - Maintenance Vendor Name
   - Maintenance Help Desk Phone Number
   - Indication of Existing Warranty or Maintenance Contract
   - Maintenance Contract Number
   - Level of Maintenance Purchased
   - Period of Performance (POP) Dates

   DISA will monitor warranty/maintenance contract expiration dates as well as End-of-Life (EOL) timeframes for the asset, and will notify partners in writing within 180 days of

expiration. This contact will initiate discussion between DISA and the partner to determine one of the following methods for dealing with maintenance expiration:

- Partner intends to provide their own extended maintenance on the hardware.
- Partner intends to provide their own technical refresh for the hardware that has reached EOL.
- Partner requests DISA acquire the necessary hardware for technical refresh through capacity services contracts.

DISA will only provide maintenance support for partner-owned assets when all of the following conditions are met:

- Current DISA contracted vendors are able to support the asset.
- EOL dates for the asset are more than 18 months away
- Partner agrees to fund the annual maintenance costs documented in the DISA cost estimate (either LE or PE)
- Asset must remain on DISA's maintenance contract for a minimum of 12 months

DISA does not provide property accountability services for partner or vendor-owned assets. It is incumbent upon the owner of the assets to meet all DoD regulatory or partner-specific property accountability guidance that may apply. DISA shall track partner/vendor-owned assets for contractual purposes only in the IT Service Management – Change Configuration, and Asset Management (ITSM-CCA) tool and shall annually inventory partner/vendor-owned property. Partner/vendor property custodians, upon request, may request current partner/vendor-owned inventory reports.

3) Software – DISA must acquire, own and maintain all executive software. Application software, unless otherwise discussed below or for solutions under our "As a Service" model, is owned by the partner. The partner is responsible to abide by all license terms and conditions imposed by End User License Agreement (EULA). The partner is responsible for the license management and any/all compliance issues that might arise. If the partner is proposing to provide their own executive software, the executive software licenses must be transferred to DISA. No executive software is permitted to operate on a DISA mainframe or server that is not DISA-owned.

   a) Executive Software

      i) Scope – for purposes of DISA software management, the scope of executive software has been defined as: The basic OS, utilities, tools and other commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) software products used to control and manage the execution of applications and their interaction with the hardware configuration. Executive software allows the processing of specified data against an application to produce the intended results.

      ii) Management – DISA shall perform installation, maintenance, and technical support for executive software packages. DISA shall maintain the most current version, licensing documentation, and release levels acquired under existing contract maintenance terms. DISA shall apply service packs, hotfixes, security releases and other patches as appropriate. Activities related to the sustainment of executive software shall be coordinated with the partner.

   b) Application Software

i) Mainframe (IBM or Unisys) – On behalf of the partner, DISA shall procure the necessary executive software to allow the application software to run, and shall charge the partner directly for the cost.

ii) Server – Any application software that is not bundled in the server rate shall be directly charged to the partner.

c) Software Transfers

i) Mainframe – Mainframe software is not generally transferable unless approved by the software vendor.

ii) Server – Server software is generally transferable with vendor approval. It is the responsibility of the current owner to provide proof of ownership and to ensure that licenses are transferable. Any fees associated with a contract/Agency transfer shall be charged to the partner accordingly. The licenses must be under a current maintenance agreement and the use must be in accordance to the vendor's current EULA.

iii) Client Access Licenses (CALs) – A CAL is a software license that allows end users to connect with server software to use the software's services and various applications. As such, CALs are considered application software, unless otherwise discussed or for solutions under our "As a Service" model, which are owned and maintained by the partner. For Enterprise Services, management of CALs will be addressed by the program management office (PMO) on a case-by-case basis.

iv) If the partner is proposing to provide their own software for transfer to DISA, the following guidelines are required to ensure that appropriate, uninterrupted maintenance support is provided for the software. The following items are required in order to effect the transfer:

(1) A completed, signed Software Transfer Agreement (Appendix B) submitted to DISA.

(2) A completed table of data elements for each software license/maintenance agreement being transferred.

(3) Originals or copies of all documentation that establishes/demonstrates proof of ownership for the software to be transferred. Certificates of ownership/origin, vendor-accepted contracts or delivery orders, purchase invoices, and/or maintenance renewal invoices are acceptable proofs of ownership.

(4) Any media containing original or backup copies of the software, which could be of use to DISA.

(5) For software currently covered under a renewable maintenance contract, the partner shall notify the applicable DISA CAR to change the address for renewal notification.

11.0 Security and Access

1) Information Systems
   a) Information systems hosted within DISA environments must maintain compliance with DoD and Joint Staff regulations, US CYBER Command directives and guidelines, and other proper authority. (See Appendix F – References.)
   b) Information systems must have a current Authority to Operate (ATO) or Interim Authority to Test (IATT) to enter DISA production environments. Systems operating with IATT shall not be used for operational purposes. (Ref. DoD 8510.01)
   c) DISA will accept Certificates of Networthiness (CoN) for partner applications hosted in DISA computing facilities under the following conditions:
      i) The CoN is signed by the partner AO or service-level CoN-issuing authority.
      ii) The CoN data is accurate based on the original networthiness assessment and may be leveraged or reused to support assessments by DISA.
      iii) The CoN affirms the fact that the application has gone through a security review and is in compliance with the DoD Application Security and Development STIG.
      iv) The application does not adversely affect the security posture of the underlying OE which includes all components below the application level (i.e., OS, middleware, web and database servers).
      v) The partner does not require administrative privileges to the underlying OE.
      vi) The partner does not require Configuration Management (CM) control of the underlying OE.
      vii) DISA has the ability to patch and maintain the security posture of the underlying OE without awaiting permission of the partner (Ref. DoD Memo Nov 2011).
   d) If any of these conditions cannot be met, DISA will require a copy of an existing accreditation memo such as an ATO or IATT. The accepted CoN will be appended to the hosting site's accreditation package.
   e) All information systems shall be hosted and monitored using DISA-provided capacity and DISA-supported OSs.
2) Web and application servers must be operated in separate environments from databases. Web and application servers should be separated, per the current Web, Application, and DMZ STIGs. These STIGs can be found at: http://iase.disa.mil/Pages/index.aspx.
3) A DMZ or Service Network provides enhanced security for servers that provide data to users outside of an enclave. The DMZ is a perimeter network segment that enforces the internal networks IA policy for external information exchange. Non-secure Internet Protocol Router Network (NIPRNet) DoD DMZ Policy Requirements state that connections between DoD enclaves and the Internet or other public or commercial WANs require a DMZ. Therefore, a DMZ shall be established within the security architecture to host any publicly accessible systems (e.g., FTP servers, public web servers, mail servers, external Domain Name Server [DNS], X.500 directories, etc.). All DMZ traffic shall be routed through the firewall for application-level processing and the DMZ shall be isolated from the rest of the protected network.
4) Data sharing or manipulation across partner applications is prohibited, unless agreed upon by all parties and documented in the SLA(s).

5) Destruction of storage media shall be conducted IAW DISA local policy and procedures.

6) Root Access Limitations
   a) Partner root access is only allowed when an information system is in an approved T&D environment. Partner root access shall be revoked before an information system is promoted into a DECC production environment. The partner may be granted certain limited privileged access as determined by the DISA Chief Information Officer (CIO).
   b) The partner requiring full root access to a production information system must have the application moved into a T&D environment before access is enabled.

7) Application Monitoring – Application audit logs and network traffic must be monitored IAW with STIGs. The OS administrator must have access to application logs.

8) Computer Network Defense (CND) – All information systems must maintain CND service capabilities to continuously protect, monitor, detect, analyze, and respond to unauthorized activity during all operating hours of the system.

9) Negligent Discharge of Classified Information (NDCI) – An NDCI occurs when classified information is introduced to a system above the level of classification for which the system is accredited. If a partner organization causes a spillage within a DISA-hosted environment, it shall be held financially liable and shall be billed for all accumulated restoration costs. The minimum amount charged to partners for DEE NCDIs is $2,500 per incident.

10) FISMA Reporting – RMF security status reports are used to help satisfy FISMA reporting requirements for network infrastructure assets owned and operated by DISA. DISA does not report on individual OEs or applications associated with partner workloads. The partner is responsible for their FISMA reporting.

11) Roles and Responsibilities are as defined below, unless otherwise documented in the SLA.
   a) Enterprise Services: IA, C&A/A&A, and compliance are maintained by DISA for enterprise systems wholly owned and operated by DISA and offered as a service to the partner (i.e. DEE). The partner is responsible for reporting any security incidents that affect these systems (i.e. DEE spillage).
   b) Shared Responsibilities
      i) Overall security is shared between the DISA DAA/AO and the partner DAA/AO, except when using milCloud and milCloud Plus services. When using milCloud or milCloud Plus services, the partner's DAA/AO is exclusively responsible for the security posture of the VDC. This includes the security status for the VDC and any OE that is managed by DISA.
      ii) IA and Compliance Validation of information systems hosted within DISA environments are shared between DISA and the partner. The DoD Technical Advisory Group (TAG) has identified typically Inherited IA Controls which DISA has adopted and abides by. Partners will inherit those IA controls based on the information system's MAC and Confidentiality levels. These controls are outlined in the attached IA Controls documents by MAC and Confidentiality level (see note below).

iii) The DoD TAG has identified Negotiable IA Controls which DISA has adopted and abides by. Partners are responsible for the negotiable IA controls based on the information system's MAC and Confidentiality levels unless vetted and approved by the DISA Cyber Assurance Branch. Any exceptions will be explicitly documented in the SLA. These controls are outlined in the attached IA Controls documents by MAC and Confidentiality level (see note below).

iv) The DoD TAG has identified Program-Owned IA Controls. These controls are the sole responsibility of the partner and are based on the information system's MAC and Confidentiality levels. These controls are outlined in the attached IA Controls documents by MAC and Confidentiality level (see note below).

NOTE: To access these IA Control documents, please click on the paperclip icon to the left and double click on the attachment you would like to view. In order to view the paperclip icon, you may have to select "Trust this Host" under the Options tab or "Enable All Features" in the pop-up banner.

v) CND is shared between DISA and the partner as documented in Appendix C – Computer Network Defense.

c) DISA Responsibilities

i) IA for DISA's accreditation boundary which includes network and facility infrastructure, enterprise programs, and internal systems. DISA certifies to the partner that the required security mechanisms are present and operational IAW DoD and Joint Staff regulations and US CYBER Command directives and guidelines.

ii) Maintaining security compliance for all DISA-hosted OSs as approved by the partner.

iii) Fully implementing the Typically Inherited IA Controls IAW the DoD TAG.

iv) Maintaining a Personnel and Information Security Program to ensure access is in accordance with applicable DoD security directives.

v) Maintaining a system for managing access control to the OS and its supporting utility software.

vi) Applying all Continuous Monitoring Risk Scoring (CMRS) System-related security fixes and vendor-recommended software maintenance to all OEs and applications managed by DISA and approved by the partner.

vii) Incident Reporting

(1) Notifying the partner of any suspected or known security deviations or violations.

(2) Immediately directing any security incidents through DISA security channels and notifying the partner (if affected by the incident).

viii) C&A/A&A

(1) Maintaining accreditation/authorization decisions for DISA network and facility infrastructure, enterprise programs, and internal systems IAW DoD 8510.01.

(2) Upon request, providing a copy of the hosting DECC's DAA/AO-signed accreditation memo and DIACAP Scorecard to the partner to validate satisfaction of controls for which DISA has responsibility.

(3) Providing IA consulting services for C&A/A&A and CMRS issues.

(4) Documenting COOP responsibilities assigned to DISA, developing recovery processes to be executed by DISA, and participating with the partner who pays DISA for COOP services in COOP exercises of those processes.

ix) Application Monitoring – If DISA manages an application, DISA shall provide monitoring of application audit logs and network traffic IAW STIGs.

x) CND – DISA provides certain Tier 3 CND capabilities 24 hours a day as described in Appendix C – Computer Network Defense.

xi) Other Compliance Issues – DISA shall implement an acceptable Risk Management Plan, and any other applicable Federal, Departmental and/or Agency policies, guidelines or requirements that are provided in writing by the partner (i.e. Common Criteria, Health Insurance Portability and Accountability Act [HIPAA], Privacy Act).

d) Partner Responsibilities

i) CMRS and Enterprise Mission Assurance Support Service (eMASS) data entries for the partner's information system. Additional information regarding user IDs/passwords, PKI certifications, and online training for CMRS can be located at the following link: https://powhatan.iiie.disa.mil/vulnerability-mgmnt/documentation/index.html.

ii) The partner's Program Manager (PM) is responsible for following Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01. The PM shall monitor and respond to IAVMs, STIGs, and Security Requirements Guides (SRGs). The PM shall provide DISA with a fix action plan, software release, or a Plan of Action and Milestones (POA&M) with mitigation plan. The PM should monitor the application security patches from the vendor and provide releases to DISA. Security patches from the vendor should be no more than one (1) generation old.

iii) The partner's PM shall review and respond to any IA related change requests initiated by DISA. In the event the partner non-concurs with an IA change request, the partner shall provide, via their DAA/AO, full specific documentation on why they are non-concurring with the change request. Such documentation shall provide the complete and specific actual problem(s) that would be introduced by implementing the IA change, any potential suggested alternatives, alternative dates for implementing the IA change, etc. This is required at the time the change request is non-concurred. Failure to provide specific and detailed documentation for the non-concurrence of an IA change request shall result in the approval and implementation of the change request. The partner's PM shall provide a complete and full copy of the documentation (as provided to the partner's DAA/AO) to the DISA operational site from where the IA change request originated. Such documentation shall be provided concurrently to DISA and the partner's DAA/AO.

iv) Security tasks related to information system components that DISA is not contracted to support. (This includes, but is not limited to, database administration, web administration, and application support.)

v) Ensuring control of all data retrieved from within DISA technical environments and for the security of any and all partner-owned and controlled technical environments. Partners shall provide certifications to DISA that their security mechanisms are present and operational.

vi) Incident Reporting

(1) Partners shall notify DISA of any suspected or known security deviations or violations involving systems hosted with DISA.

(2) Partners shall immediately direct any security incidents through partner security channels and DISA (if affected by the incident).

vii) Obtaining an updated accreditation/authorization decision when workload (new or amended) is implemented within a DECC. If an updated accreditation cannot be obtained within 90 days of FOC, the partner program Information System Security Manager (ISSM) will provide the plan and timeframe to achieve C&A/A&A. This document must be signed by the partner's AO or representative.

viii) Application Monitoring – Partners shall monitor application audit logs and network traffic IAW STIGs, unless DISA application management services are provided.

ix) CND

(1) Partners are responsible for ensuring comprehensive CND services exist and are operational.

(2) Partners are responsible for all CND services not explicitly provided by DISA.

x) Other Compliance Issues – Partners shall provide written identification of all Controlled Unclassified Information applications and information being processed for them by DISA, and the required protection during transmission.

xi) Developing applications that interface and exchange identification and authentication with the security products utilized by DISA and the DoD-sanctioned STIGs and Application IA Controls IAW NIST 800-53 v4.

xii) Partners with authority to add, delete, change, and unlock locked system accounts agree to maintain a copy of the DD Form 2875 for each active user. They also agree to provide a copy of the DD Form 2875 upon request to DISA.

xiii) Coordinating with DISA on any Exceptions to Normal Processing as soon as they become known. DISA shall respond to partner requests for Exceptions to Normal Processing within 10 calendar days after formal notification. Exceptions to Normal Processing are defined in the Glossary. Normal Processing services are specified in the SLA.

xiv) Furnishing both the primary and alternate partner POCs to the DISA Service Desk, and updating as necessary. In the event the Service Desk cannot contact the primary POC, the alternate on the list shall be contacted. The partner POC shall notify the partner users of any operational situations that impact service.

xv) Coordinating with DISA representatives to prioritize the partner's applications and to develop the COOP plan.

xvi) Maintaining access control for users to their applications.

xvii) Furnishing all notifications and information to DISA via memorandum or electronic mail; and by telephone, if urgent, to confirm receipt.

xviii) Making appropriate modifications to applications in support of periodic executive software and hardware upgrades.

xix) Partner applications referring to hard-coded IP addresses must be changed to DNS addresses where possible.

xx) Allowing DISA sufficient administrative rights and privileges to apply all CMRS-related security fixes and vendor-recommended software maintenance to partner-owned equipment residing in DECCs.

NOTE: DISA policy states that DISA shall no longer accept partner-owned equipment after the first of October, 2011. Partner-owned equipment currently residing in DECCs shall be grandfathered until end-of-life and technical refresh. (Ref. Section 10.0 Ownership and Licenses)

xxi) Providing the following IA information for the partner's information system and applications and notifying DISA in writing of any changes to this information.

(1) Certifiers Recommendation Statement and Accreditation Decision

(2) Partner AO risk acceptance for residual risk memorandum

(a) Documented Risk Acceptance (DRA)

(b) Plan of Action and Milestones (POA&M) identifying any open vulnerabilities

(3) An Application Security Review Checklist and Application STIG results for:

(a) Database (if partner-owned)

(b) Web (if partner-owned)

(c) Application (if partner-owned)

(4) Compliance Assessment IAVM and Reporting must be completed. Security Test and Evaluation (ST&E) must be completed if required.

(5) Implementation of and compliance with IAVMs, STIGs, SRGs, and Communications Tasking Orders (CTOs) for their accredited/authorized information systems and applications.

(6) Ports, Protocols, and Service Management (PPSM) Registration

(a) The partner shall register all ports, protocols, and services for the partner's information systems via https://pnp.cert.smil.mil. *NOTE: This is a Secure Internet Protocol Router Network (SIPRNet) link.*

(b) The partner shall provide DISA with the partner's confirmation e-mail from PPSM

(c) Unidentified ports shall be accompanied with pertinent mitigations

(7) Registration in the following authoritative data sources: DoD IT Portfolio Repository (DITPR), CMRS, eMASS, PPSM, etc.

12.0 Additional Responsibilities

1) DISA shall determine hosting and management sites.
2) The partner shall submit any specialized or additional communications support requirements 120 calendar days in advance for Automated System Interruption (ASI) and 7–10 business days for general requirements. Urgent requirements shall be handled on a case-by-case basis. All ASI requests must be submitted to the supporting Service Desk.
3) The partner shall test all new releases prior to releasing into the production environment. The partner shall release testing to DISA if requested.
4) DISA shall notify the partner of:
   a) Changes to established hours of processing or service availability
   b) Scheduled downtimes or other restrictions to processing or service availability, at least 72 hours in advance
   c) Hardware and software upgrades, releases, and changes which may impact the partner
   d) Any suspected or known security deviations or violations
5) Any request for auditing of business, financial, or medical systems will be coordinated and supported by Mission Assurance Cyber Services. To ensure timely service delivery, partners must note requirements early on in the request fulfillment process and provide advance notification 90 days prior to any auditing related event.

13.0 Dispute Resolution

An alternative Dispute Resolution clause is as follows:

1) Dispute resolution shall involve the program offices, resource management office, accounting offices, KO, and agency's Chief Financial Officer (CFO), as appropriate. Disputes shall be documented in writing with clear reasons for the dispute. A Memorandum of Agreement (MOA) shall be signed by the CFOs of each department and agency to acknowledge the active participation of that department or agency in the dispute resolution process.
2) Trading partners shall not chargeback or reject transactions that comply with these rules. Further, new transactions shall not be created to circumvent these rules. Transactions that comply with these rules, but are disputed, shall be resolved as delineated in the following paragraphs. Disputes are of two types: accounting treatment (e.g., of advances, non-expenditure transfers) and contractual (e.g., payment, collection, interagency agreement).
    a) If Intragovernmental differences result from differing accounting treatment, the trading partners have 60 calendar days from the date a charge is disputed to agree on the treatment of an accounting entry. If agreement cannot be reached, both trading partners' CFOs shall request that the CFOs Council's Intragovernmental Dispute Resolution render a final decision.
    b) If Intragovernmental differences result from contractual disputes, the trading partners have 60 calendar days from the date a charge is disputed to agree on the contractual terms. If agreement cannot be reached, both trading partners' CFOs shall request that a binding decision be rendered by the CFOs' Council's Committee established for this purpose. The Committee shall render a decision within 90 calendar days of request. The trading partners shall then coordinate to ensure any necessary IPAC transaction needed to effect the decision is processed as applicable.
    c) Missing indicative data on an Intragovernmental transaction is cause for a contractual dispute. The partner may establish a monetary threshold before asking for contractual decisions; the threshold shall not exceed $100,000 per order. If an amount is under the partner's threshold, and the partner elects not to pursue a dispute, then the partner shall pay the amount.

When it appears that an SLA has been breached by either party, DISA shall identify the circumstances behind the incident. The resolution could take many forms (i.e. a Service Improvement Plan [SIP] that is referred to the DISA Problem Management team or a modification to an SLA).

Appendix A – Termination Worksheet

To access this form for use, please click on the paperclip icon to the left and double click on the Termination Worksheet attachment. *NOTE: In order to view the paperclip icon, you may have to select "Trust this Host" under the Options tab or "Enable All Features" in the pop-up banner.*

1) With the assistance of the DISA CAR, the partner shall provide this completed worksheet if one of the following occurs:
   a) The partner is eliminating DISA support/entire SLA.
   b) The partner is decommissioning an entire application/ASC.
2) This worksheet is not needed, but the partner must still provide written notification (i.e. an e-mail) to DISA, if:
   a) The partner is discontinuing an existing optional service such as database administration or application support, but not all support for an application/system.
   b) The partner wants to de-install existing hardware, but not an entire suite of hardware or application/system. In this case the partner will open a ticket with their supporting DECC service desk and notify their CAR.

DISA Termination Worksheet	
Customer Name:	
Email:	
1. Application System Code (ASC):	
2. Data System Designator (DSD) if applicable:	
2.a. If this covers only a partial DSD please explain:	
3. System Name:	
4. System Location:	
5. Shutdown date by site (This date will deactivate processing capabilities. The system will be idled, but data will be kept intact and the ability to bring back online as a backup or fail measure is still an option. Storage of these files will incur machine utilizations costs until final shutdown. If needed, additional dates and sites can be provided.):	
Date(s):	**Site(s):**
Date(s):	**Site(s):**
Date(s):	**Site(s):**
Date(s):	**Site(s):**
Date(s):	**Site(s):**
6. Final Decommission date by site (This is the date that officially shuts down all files and storage capability unless specific arrangements are requested in item 12):	
Date(s):	**Site(s):**
Date(s):	**Site(s):**
Date(s):	**Site(s):**
Date(s):	**Site(s):**
Date(s):	**Site(s):**
7. Replacement Automated Information System (AIS) if any:	
8. Replacement System Name:	
9. Interfacing System/s and impact:	
System(s):	**Impact(s):**
System(s):	**Impact(s):**
System(s):	**Impact(s):**

DISA Termination Worksheet	
System(s):	**Impact(s):**
System(s):	**Impact(s):**
10. Coordinating System POC (name and phone number):	
11. Date Coordinating System POC notified:	
12. High Level Qualifiers for data deletion (This input mandatory for IBM - Minimum of two. Identify as applicable):	
12a. IBM Accounts:	
12b. Unisys Accounts:	
12c. Server Accounts:	
Archiving Files Special Instructions	
13. Do you want to delete or archive datasets?	
14. High Level Qualifiers used for archiving:	
15. Organization to perform the archive:	
16. Organization to maintain the archive:	
17. Identify bill payer and Billing Account Number (BAN):	
18. Identify production jobs to be removed from the schedule:	
19. Identify any software unique to this ASC/DSD that is no longer needed:	
20. Identify other billable items for which service is no longer required such as Certification Authority (CA) Dispatch prints, special reports, etc:	
21. Identify retention requirements with media and data set name if different than listed in item 14 above:	
22. Shipping address where archived files are to be sent/returned for storage:	

DISA Termination Worksheet	
Authorization Signatures:	
23. Functional Owner	
Name:	Office Symbol:
Phone:	Fax:
E-mail:	
Signature:	Date:
24. Engagement Executive Team	
Name:	Office Symbol:
Phone:	Fax:
E-mail:	
Signature:	Date:
25. Resource Management	
Name:	Office Symbol:
Phone:	Fax:
E-mail:	
Signature:	Date:
26. Operations	
Name:	Office Symbol:
Phone:	Fax:
E-mail	
Signature:	Date:
27. (Other – as required)	
Name:	Office Symbol:
Phone:	Fax:
E-mail	
Signature:	Date:
28. (Other – as required)	
Name:	Office Symbol:
Phone:	Fax:

DISA Termination Worksheet	
E-mail	
Signature:	Date:
Any questions regarding this form can be directed to the Engagement Executive. POC: DSN:	

Appendix B – Software Transfer Agreement

To access this form for use, please click on the paperclip icon to the left and double click on the Software Transfer Agreement attachment. *NOTE: In order to view the paperclip icon, you may have to select "Trust this Host" under the Options tab or "Enable All Features" in the pop-up banner.*

(Partner) agrees to transfer ownership of all rights associated with the software specified in the below table(s). (Partner) acknowledges that it is the rightful owner of this software, and that transfer to DISA is permissible under its licensing agreements for the specified software. To the maximum extent possible, (partner) agrees to provide proof of ownership for all listed software. If applicable, (partner) agrees to notify software vendors that future license maintenance renewals are to be sent to DISA.

Data Element	Asset Description
Vendor	
Vendor POC	
Product Name	
Number of Licenses	
Product Number	
Version	
Maintenance Expiration Date	
Pass Codes/ Keys	

The official signature affixed below reflects understanding and indicates approval by the partner to the requirements and terms and conditions of this Agreement.

For the partner: (Authorizing Official)

Signature: _____

Date: _____

Printed Name: _____

Title: _____

Appendix C – Computer Network Defense

The roles and responsibilities detailed below apply only to those partners that have elected DISA to serve as the Cybersecurity Defense Service Provider (CDSP) for their programs/applications. For partners' programs/applications that reside within a DECC but have not aligned with DISA as their CDSP, notification of suspicious traffic observed by Columbus Network Assurance (COLS-NA) will be supplied to the applicable CDSP via Tipper and subsequent CDSP actions will be performed by the partner CDSP.

For partner programs/applications that have traditionally received any of the functions detailed below by DISA, but are not aligned in writing with DISA, please coordinate with CDSP Requests (DISA Letterkenny AD RE List CDSP Requests disa.letterkenny.re.list.cdsp-requests@mail.mil) to have that documented appropriately.

DISA employs a documented reporting structure designed to facilitate sharing and collaboration of information among all stakeholders involved with defense of the Department of Defense Information Network (DoDIN). This reporting structure is also leveraged to alert mission owners of cyber incidents and to disseminate information in order to mitigate or correct conditions associated with that event. The success of the CDSP program relies heavily on timely collation, correlation, information analysis, and warning dissemination. Additionally, automated analytical tools and alerts of attacks in progress are essential to the CDSP process. This reporting structure shall also be linked to intelligence, law enforcement, policy makers, and the Regional or Theater-level information systems community (both government and commercial). Coalition Network Operations (NetOps) Centers (CNCs)/Theater NetOps Centers (TNCs) incident reporting procedures shall consider the information needs of the intelligence and operations communities for planning, coordinating, and implementing response options.

The following information outlines the CDSP roles and responsibilities for both the provider (DISA) and mission partners that have aligned to DISA as their CDSP. The partner SLA should clearly indicate whether the partner has aligned to DISA as their CDSP.

NOTE: CDSP services not provided to the partner by DISA either due to the partner declining that service (documented in SLA Attachment A Validation Letter) or technological, staffing, or mission infeasibility, should be performed by the partner themselves or by their Component head.

1) Malware Notification Protection (MNP)

a) Service POCs: DISA Command Center-Network Assurance
   i) DISA Ft Meade Operations (OPS) Mailbox DISA Command Center Network Assurance Watch Office (DCC-NAWO) disa.meade.ops.mbx.dcc-nawo@mail.mil
   ii) DISA Ft Meade OPS Mailbox DCC-Battle Captain (BC) disa.meade.ops.mbx.dcc-bc@mail.mil

b) Description: MNP is the processes by which the CDSP alerts partners to new malware and assists the partner when an incident occurs. The CDSP maintains contact with anti-malware software vendors so that effective countermeasures are developed, tested, and deployed as quickly as possible.

c) Services Provided

i) Access to anti-virus/anti-malware software
ii) Access to updated signatures for NIPRNet and SIPRNet
iii) Warnings and updated information on malicious threats
iv) Access to 24x7 virus response capability and the ability to request support
v) Ability to create custom detection capabilities with enterprise tools

d) Roles and Responsibilities

i) DISA will:

(1) Provide access to anti-virus/anti-malware software and updated signatures for NIPRNet and SIPRNet. Through subscription to the Net Defense virus list server, and other anti-virus organizations, provide warnings and updated information on malicious (spyware, viruses, malware, adware, etc.) code threats.

(2) Maintain a 24x7 virus response capability and respond to all partner reports of virus activity or requests for support.

(3) Maintain a current POC list for DoD-approved vendor support.

(4) Implement formal procedures to report emerging viruses to United States Cyber Command (USCYBERCOM) within reporting time requirements.

(5) COLS-NA will incorporate already established Host Based Security System (HBSS) feeds into the analyst toolset for monitoring purposes once the partner has established an HBSS presence.

(6) Ensure proper protection of data in transit, in accordance with DoD policy.

ii) The partner will:

(1) Ensure all components implement anti-virus/anti-malware (e.g. HBSS) software and maintain updated signatures for all NIPRNet and SIPRNet systems.

(2) Communicate HBSS alerts to COLS-NA for incident handling action.

(3) Maintain responsibility for compliance with USCYBERCOM requirements

(4) Conduct weekly anti-virus scans of network-connected devices in accordance with the DoD STIGs; develop/implement a program to identify infected assets; and rebuild, quarantine, or remove the asset from the network upon detection.

(5) Ensure all CND personnel are aware of DISA's 24x7 capability to assist with malware mitigation and maintain an up-to-date listing (NIPRNet/SIPRNet email, phone, secure phone, etc.) for contacting DISA.

(6) Ensure personnel understand how to conduct timely reporting of the detection of unknown/emerging malware to DISA.

(7) Work with DISA to obtain Reverse Engineering/Malware Analysis (RE/MA) support if malware is identified (reference Incident Response – Analysis section for additional information)

2) Mission Partner Support and IA Training (S&T)

a) Service POCs

i) Support/Questions/Change Requests disa.letterkenny.RE.list.cdsprequests@mail.mil
ii) Training disa.letterkenny.RE.list.training-team-members@mail.mil

b) Description: Mission Partner Support and IA Training is essential to initiating and maintaining the Cybersecurity Defense (CD, formerly CND) services for new or existing partners. This support includes the coordination of the initial request for services, support agreements and funding, maintenance of partner configuration information, coordination and de-confliction of external assessments, and CDSP programmatic sustainment activities identified by DoD Directive (DoDD) O-8530.2. This also includes high-level coordination and support for CDSP partner IA/CD training requirements to include: providing assistance in acquiring IA education and training, and spreading knowledge and awareness throughout the DoD.

c) Services Provided

i) Assistance with identifying CD, NetOps and IA training requirements, upon request
ii) Vulnerability alerts and timely technical solutions/assistance – Annual general and specific network hardening guidance
iii) Access to NetOps and IA computer based training (CBT) courses

d) Roles and Responsibilities

i) DISA will:

(1) Assist the partner with identifying CD, NetOps, and IA security training requirements, upon request

(2) Maintain configuration documentation received for partner networks to include: network diagrams, technical sensor/administrative, and policy POCs and related information.

(3) Alert the partner to vulnerabilities and provide timely technical solutions/assistance. Provide general and specific guidance on the hardening of the partner network components via STIG release.

(4) Work with Education, Training, and Awareness (ETA) providers to incorporate CD requirements into ETA curricula and courseware and provide course development technical support in the areas of network

protections, malicious code, Information Operations Condition (INFOCON)/Cyber Operations Condition (CYBERCON) and IAVM.

(5) Notify the partner of any CM changes or changes/activities that could affect NetOps.

(6) Share sanitized partner data and items of interest with the network assurance community.

ii) The partner will:

(1) Maintain, and provide to DISA upon request, accurate CM documentation as required. Documentation that has been reviewed within the last year to include (but not limited to): network diagrams, software and hardware inventories and network ports, protocols and services (PPS) listing, technical sensor/administrative and policy POCs lists and related information.

(2) Provide situational awareness to DISA of any known vulnerabilities, mitigation strategies, major changes to the network, or other actions that would affect DISA's ability to protect partner networks.

(3) Maintain DISA guidelines for the hardening of networks (e.g. STIGs) and inform DISA of any significant changes to the security or architecture of the networks (e.g. architecture redesign, addition/removal of critical servers or infrastructure, etc.).

(a) Refer to the IA Support Environment (IASE) for network hardening guidelines: http://iase.disa.mil.

(b) Inform DISA of any changes by sending an email to DISA.letterkenny.RE.list.cdsp-requests@mail.mil.

(4) Identify and provide asset data on critical network assets (servers, security devices, network devices, DNS, Primary Domain Controllers [PDCs], Backup Domain Controllers [BDCs], etc.) so DISA can more accurately assess risk to those assets.

(5) Notify DISA of any CM changes involving connectivity, to include location, sensor name, Command Communication Service Designators (CCSDs), bandwidth, IP address space, and/or backend connections or changes that could affect NetOps.

Inform DISA of any changes by sending an email to DISA.letterkenny.RE.list.cdsp-requests@mail.mil.

This information should be provided to:

NIPR: DISA.letterkenny.RE.mbx.CDSPsubmission@mail.mil

SIPR: DISA.letterkenny.RE.mbx.CDSPsubmission@mail.smil.mil

3) INFOCON Compliance/NetOps Awareness

a) Service POCs: General questions can be directed to

DISA.letterkenny.RE.list.cdsp-requests@mail.mil

b) Description: INFOCON Compliance/NetOps Awareness involves the monitoring of the CDSP partner's INFOCON level, providing technical subject matter experts (SMEs) to the commander, as requested, to assist with determining INFOCON measures, and tracking and reporting INFOCON compliance.

c) Services Provided:

i) Monitoring the CDSP partner's INFOCON level
ii) Providing technical SMEs to the commander, as requested, to assist with determining INFOCON measures
iii) Tracking and reporting INFOCON compliance
iv) Guidance and assistance as required/requested.

d) Roles and Responsibilities

i) DISA will:

(1) Maintain the latest DoD guidance and procedures for the INFOCON/ CYBERCON reporting process, formats, directive actions, and security.

(2) Provide notification to the partner of all changes to the global and theater (where appropriate) INFOCON/CYBERCON level, and recommend actions in response to any changes to the INFOCON/CYBERCON level or Targeted Response Options (TROs). Monitor partner INFOCON/CYBERCON status, and advise USCYBERCOM of any changes.

(3) Provide guidance at least annually to the partner on directed measures to protect their networks in response to INFOCON/CYBERCON levels 5 through 1.

ii) The partner will:

(1) Ensure all partner organizational elements implement appropriate INFOCON/CYBERCON levels. Immediately notify DISA of any partner-directed change in INFOCON/CYBERCON level or TROs.

(2) Maintain the latest DoD guidance and procedures for the INFOCON/ CYBERCON reporting process, formats, directive actions and security.

(3) Provide a read-only view in DoD approved vulnerability repository of assets and POC information to DISA for situational awareness of vulnerability status and mitigation strategies.

4) Information Assurance Vulnerability Management (IAVM)

a) Service POCs: General questions can be directed to DISA.letterkenny.RE.list.cdsp-requests@mail.mil

b) Description: USCYBERCOM directly alerts all Combatant Commands, Services, DoD Agencies (C/C/S/As) and Field Activities of new/emerging threats and vulnerabilities.

DISA manages the IAVM system for DoD, but additionally monitors CDSP partner implementation of and compliance to IAVMs, generates IAVM assessment reports, and provides technical support to partners as required.

c) Services Provided:

i) Monitoring CDSP partner implementation of, and compliance to, IAVMs
ii) Generating IAVM assessment reports
iii) Technical support to partners as required
iv) Guidance and assistance as required/requested

d) Roles & Responsibilities

i) DISA will:
(1) Analyze feedback received on the relationship between IAVM status of partner assets and any malicious incidents that occur.
(2) Provide feedback and recommendations to the partner.

ii) The Mission Partner will:

(1) Maintain compliance with IAVM program directives and vulnerability response measures.

(2) Ensure the proper acknowledgement and reporting of IAVM notices via generated messages. Appropriate personnel (e.g. IA Manager [IAM], ISSM, SA, etc.) must have and maintain active accounts in a DoD approved vulnerability repository.

(3) Establish a comprehensive Vulnerability Management Plan, including vulnerability remediation, STIG compliance management, and patch testing.

(4) Provide feedback to DISA on the relationship between the IAVM status of assets and any malicious incidents that occur.

5) Network Security Monitoring (NSM)/Intrusion Detection

a) Service POCs:

i) General questions: DISA.letterkenny.RE.list.cdsp-requests@mail.mil
ii) COLS-NA: disa.columbus.eis.mbx.cols-esdna@mail.mil

b) How to Request: To request additional NSM support contact DISA.letterkenny.RE.list.cdsp-requests@mail.mil

c) Description: NSM includes the monitoring of sensors that detect attacks on the DoDIN. This is accomplished through the monitoring of partner networks to detect unauthorized activity via Intrusion Detection and Prevention Systems (IDPS) and determining if network and host activity is intrusion related. The IDPS-derived information provides analysts with technical event and incident data to process into intrusion analysis, correlation, and reporting.

d) Services Provided: Monitoring of unclassified and classified network CCSDs/IPs using approved sensors via the assigned DISA NetOps Center (DNC).

NOTE: For mission partners, COLS-NA will be the monitoring center.

e) Roles and Responsibilities

i) DISA will:

(1) Utilize formal network security monitoring policies and procedures that include the appropriate use of DoD-approved IDPS tools that have automated alert capabilities enabled.

(2) Perform detection (monitoring and analysis) activities on the CCSDs or IP space/range if CCSDs aren't applicable, using intrusion detection sensors/intrusion prevention sensors (Intrusion Detection System [IDS]/ Intrusion Prevention System [IPS], hereafter called sensors. Activity will occur on a 24x7 basis via the DNCs/COLS-NA.

(3) Follow documented procedures for characterizing anomalous events detected by sensors and other network monitoring systems.

(4) Monitor the partner's unclassified and classified networks. Provide CDSP failover COOP in the event of an outage at the service provider location.

(5) Review and analyze logs in a timely manner to detect intruders, and within 30 minutes of detection of an event, begin preliminary analysis of the event. Follow documented procedures to obtain copies of partner audit/system logs.

(6) COLS-NA will incorporate already established HBSS feeds into the CDSP analyst toolset.

ii) The partner will:

(1) Develop a local AO-approved program to utilize approved network security monitoring tools.

(2) Ensure all components implement anti-virus/anti-malware (e.g. HBSS) software and maintain updated signatures for all NIPRNet and SIPRNet systems.

(3) Develop and maintain documented policies and procedures for assessing baseline configuration guidelines, and maintaining the continued update of security standards.

(4) Provide audit/log files to DISA as requested for correlation activities.

(5) Aid DISA in determining the optimum location of sensors. Provide DISA with unclassified and classified network topology diagrams representing all enclaves being monitored. The partner/DISA will mutually agree on sensor placement.

(6) Ensure sensors purchased are the size/model recommended by DISA.

6) Attack Sensing and Warning (AS&W)

a) Service POCs: COLS-NA disa.columbus.eis.mbx.cols-esdna@mail.mil

b) Description: AS&W is the collection, normalization, and correlation of event incident data to identify intentional unauthorized activity across a large spectrum, including computer intrusions or attacks, coupled with the notification to Command and Control and decision makers in order to develop an appropriate response. AS&W senses changes in partner computer networks based on the analysis of current and archived security information. This data comes from all available sources including but not limited to: device logs, security application logs, incident tickets, archives, etc. Data from other CDSPs and partners is correlated to provide more comprehensive AS&W. This type of analysis requires highly skilled CD analysts and hinges on collaboration with all tiers of the CD hierarchy.

c) Services Provided:

i) Notification of suspicious/malicious network traffic or potential computer attacks
ii) Limited impact assessments and configuration recommendations and/or rule sets based on threat data
iii) Upon identification, analysis of low-level (“low and slow”) events to identify unauthorized activity utilizing exploratory problem-solving or self-learning techniques
iv) Best practice guidance (distributed annually)

d) Roles and Responsibilities

i) DISA will:

(1) Provide notice of suspicious/malicious network traffic or similar activities that suggest an impending or on-going attack. General warnings of potential computer attacks will also be provided to the partner. Limited impact assessments and recommendations to configurations and/or rule sets may be provided based on threat data.

(2) Search for and analyze low-level (“low and slow”) events to identify possible unauthorized activity using exploratory problem-solving or self-learning techniques. Suspicious/significant activity will be shared among the CND/IA community.

(3) Distribute documented guidance on an annual basis of best practices that support an overall DoD policy for configurations or rule sets.

(4) Follow documented procedures to collaborate with other CDSPs to compare and exchange notes, analysis reports, and other information on intrusions, attacks, or suspicious activities.

(5) Provide Intrusion Assessment support for identified suspicious/malicious activities that are indicative of a compromise without a confirmed compromise.

(6) Share sanitized partner data collected with the NA community via secure channels.

ii) The partner will:

(1) Ensure AS&W information is appropriately disseminated within the partner and its sub-components.

(2) Acknowledge, maintain, and reference all DISA warnings and indications messages and security configuration guidance.

(3) Coordinate awareness of current activities occurring in partner environment (Red Team, incident response/intrusion assessment, law enforcement, counter intelligence, exercise, etc.) and relay in a timely manner the potential impact they may have on DISA's ability to conduct effective network defense monitoring.

(4) Share any internal or command analysis, information, or warnings pertaining to intrusions, attacks, or suspicious activities to DISA for situational awareness.

7) Indications and Warning (I&W)

a) Service POCs: COLS-NA disa.columbus.eis.mbx.cols-esdna@mail.mil

b) Description: I&W are intelligence-based activities that are intended to detect and report on time-sensitive intelligence information on foreign developments that could involve a threat to the United States military, political, or economic interests. I&W provides information on adversaries and includes forewarnings of enemy actions or intentions. The relevant I&W information relating to DoD information systems and computer networks received from United States Strategic Command (USSTRATCOM) or other intelligence sources is distributed to partners for situational awareness.

c) Services Provided:

i) Notification of suspicious/malicious network traffic or potential computer attacks
ii) Limited impact assessments and configuration recommendations and/or rule sets based on threat data
iii) Upon identification, analysis of low-level ("low and slow") events to identify unauthorized activity utilizing exploratory problem-solving or self-learning techniques
iv) Best practice guidance (distributed annually)

d) Roles and Responsibilities

i) DISA will:

(1) Develop tactics, techniques and procedures (TTPs) to provide the partner with intelligence-based potential computing threats and expected imminent actions on a timely basis. These warnings will be based on intelligence community and other sources. Situational awareness will also be provided to the partner based on theater activities and those threats and activities correlated from other entities (i.e., USCYBERCOM and DNCs/COLS-NA).

(2) Follow a documented methodology for sharing information with the intelligence community via proper channels, and for checking non-governmental and counterpart CDSP organizational websites for threat and warning notifications daily to ensure situational awareness.

(3) Coordinate within DISA and with the partner to consolidate and correlate situational awareness data into a single integrated picture.

ii) The partner will:

(1) Acknowledge, maintain, and reference any threat reports disseminated by DISA or other sources.

(2) Ensure I&W and situational awareness information is appropriately disseminated within the organization, and daily command situational awareness is shared with DISA.

8) Incident Reporting

a) Service POCs: COLS-NA disa.columbus.eis.mbx.cols-esdna@mail.mil

b) Description: Incident reporting is provided to CDSP partners and utilizes an incident reporting system for complete and meaningful incident report recording and rapid distribution to DoD channels and law enforcement/intelligence communities. This involves both up channel (to Tier 1) reporting on behalf of the partner and down-channel (to partner level) reporting for recovery and response actions. This additionally involves the filing and safeguarding of all incident reports so that valuable information is available for current and future analysis.

c) Services Provided:

i) Reporting incidents occurred on DISA-monitored sensors
ii) Updated incident response guidelines, checklists, and recommended procedures at least annually

d) Roles and Responsibilities

i) DISA will:

(1) Report potential incidents and correlated information from these incidents/events that occur on DISA-monitored sensors using documented procedures in accordance with DoD guidance. These events/incidents will be provided to partners and reported to USCYBERCOM.

(2) Ensure incidents are populated into the DoD enterprise incident database. DISA is the conduit to USCYBERCOM for all CND incidents.

(3) Follow documented policies and procedures for handling incidents reported to law enforcement and counterintelligence agencies.

(4) Retain all incident reports (electronic or paper) for at least one year.

(5) Share sanitized partner data collected with the NA community via secure channels.

ii) The partner will:

(1) Develop and implement a process with formal documented procedures to conduct incident handling in accordance with DoD/Chairman of the Joint Chiefs of Staff (CJCS) incident handling procedures.

(2) Self-report all incidents and questionable events for covered networks in a timely manner to DISA as discovered. DISA will enter incidents into the DoD enterprise incident database on behalf of the partner. To report an incident please contact disa.columbus.eis.mbx.cols-esdna@mail.mil. Follow documented procedures as instructed in the DISA First Responders Guide (FRG).

(3) Verify or validate incidents identified by DISA, along with any operational impact, and provide feedback to DISA in a timely manner.

(4) Retain soft or hard copies of all applicable incident reports for one year.

(5) Follow documented procedures as instructed in the FRG in coordination with COLS-NA.

DISA also offers the services detailed below, though mission partners are not automatically receiving or entitled to those services via their utilization of the DECC infrastructure. The partner's SLA/Attachment A will reflect whether any of the additional services below are applicable.

1) Vulnerability Analysis and Assessment (VAA) Support

a) Service POCs: Multiple – All requests/questions should be sent to the CDSP Requests Team at DISA.Letterkenny.RE.list.cdsp-requests@mail.mil

b) Description: VAA Support services are vital proactive activities to determine the adequacy of cybersecurity measures for DoDIN assets. Vulnerability assessments apply a variety of techniques (e.g., network discovery, network and host vulnerability scanning, penetration testing) to identify vulnerabilities and assess whether DoDIN assets conform to specific security objectives.

NOTE: As of FY16 the VAA support includes services that were previously separated under the title External Assessments.

c) Services Provided: The services annotated below are considered types of VAA Support. The individual services are described in more detail in the following sections.

i) External Vulnerability Scan (EVS)
ii) Web Vulnerability Scan (WVS)
iii) Red Team Operation (RTO)
iv) Intrusion Assessment
v) Penetration Test (Pen Test)

2) VAA – External Vulnerability Scans (EVS)

a) Service POCs: DISA Letterkenny AD RE Mailbox CNDSP VAA Team disa.letterkenny.re.mbx.cndsp-vaa-team@mail.mil

b) How to Request: Submit an email to DISA.Letterkenny.RE.list.cdsp-requests@mail.mil

c) Description: EVSs are conducted in support of, or in augmentation to, the partner's internal, DoD mandated vulnerability scanning and assessment actions. This service is provided primarily for assistance in the protection of a partner's networks and includes:

i) Identifying and testing scanning tools that can be used by the partner
ii) Assisting in the execution of EVSs to determine compliance with DoDI 8551.01 PPSM
iii) Providing bi-annual EVSs of identified targets
iv) Recommending vulnerability mitigations and strategies and assisting in false positive determination
v) Developing trends and metrics based on available vulnerability data from individual and collective partners

d) Services Provided:

i) Two EVSs per SLA
ii) Analysis and executive summary for each scan
iii) Assistance with internal vulnerability scans upon request (depending on scope, may incur additional costs)

3) VAA – Web Vulnerability Scanning (WVS)

a) Service POCs: DISA Letterkenny AD RE Mailbox CNDSP VAA Team disa.letterkenny.re.mbx.cndsp-vaa-team@mail.mil

b) How to Request: Submit an email to DISA.Letterkenny.RE.list.cdsp-requests@mail.mil

c) Description: WVS support is conducted to assist the partner in complying with USCYBERCOM (USCC) TASK ORDER (TASKORD) 13-0613 with respect to public facing web presence. This service is provided in assisting the partner in protecting DoD DMZ whitelisted web sites and includes:

i) Bi-annual scans of the partners' public facing web print with follow-on scans for the purpose of validating the partners' mitigation efforts
ii) Web vulnerability testing of all public facing websites IAW USCC TASKORD 13-0613
iii) Support to all public facing websites registered on the DoD Whitelist and will include all IPs/Fully Qualified Domain Names (FQDNs) to include: public key enabled Common Access Card (CAC), user identification and password, or no access restrictions web listings
iv) Assistance with false positive determination
v) Recommended vulnerability mitigations

vi) Developing trends and metrics based on available vulnerability data from individual and collective partners

d) Services Provided:

i) Two WVS assessment scans per SLA (NIPR only)
ii) Analysis and executive summary provided for each scan

4) VAA – Other Services

a) Service POCs: CDSP Request Team DISA.Letterkenny.RE.list.cdsp-requests@mail.mil

b) How to Request: Submit an email to DISA.Letterkenny.RE.list.cdsp-requests@mail.mil

c) Description: Optional VAA services are not required, but highly recommended.

i) Pen Test is security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. This type of testing is used to determining the effectiveness of the implemented technical security controls, in a goal-oriented, overt manner.
ii) Intrusion Assessment provides a mechanism for the hunting and eradication of previously unidentified intrusion activity on a network. The end goal of an intrusion assessment is to identify whether a network has been compromised, highlight unauthorized activity, identify any critical vulnerabilities, and provide direction to the partner for the enhancement of local Tier 3 cyber defense.
iii) RTO is a focused, threat-based operation by an interdisciplinary, simulated adversary to expose and exploit vulnerabilities as a means to develop recommendations for the improvement of the security posture and operational CD capabilities and procedures utilized to protect networks and systems.

d) Services Provided:

i) A Pen Test, Intrusion Assessment, or RTO, if purchased
ii) An after action report for any VAA completed

Appendix D – Acronyms

The following acronyms are referenced throughout this T&C.

Acronym	Definition
A&A	Assessment and Authorization
AO	Authorizing Official
AOR	Area of Responsibility
ASC	Application System Code
ASI	Automated System Interruption
AS&W	Attack Sensing and Warning
ATC	Authority to Connect
ATO	Authorization to Operate
BAN	Billing Account Number
BC	Battle Captain
BCP	Business Continuity Plan
BD	Development and Business (Center)
BDC	Backup Domain Controller
BETC	Business Event Type Code
BMMP	Business Management Modernization Program
BOM	Bill of Materials
BPN	Business Partner Network
CA	Certification Authority
C&A	Certification and Accreditation
CAP	Connection Approval Process
CAR	Customer Account Representative
CCAO	Classified Connection Approval Office
CCC	Central Communications Center
CCER	CENTRIXS Cross Enclave Requirement
CCMD	Combatant Command
C/C/S/As	Combatant Commands, Services, DoD Agencies
CCSD	Command Communication Service Designators
CD	Cybersecurity Defense
CD2	Customer Management Division
CDC	Core Data Center

Acronym	Definition
CDSP	Cybersecurity Defense Service Provider
CENTRIXS	Combined Enterprise Regional Information Exchange System
CERT	Certification
CFO	Chief Financial Officer
CIC	Customer Identification Code
CIO	Chief Information Officer
CIS	Centralized Invoice System
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CL	Confidentiality Level
CM	Configuration Management
CMRS	Continuous Monitoring Risk Scoring
CNC	Coalition NetOps Center
CND	Computer Network Defense
CNDS	Computer Network Defense Service
CNDSP	Computer Network Defense Service Provider
COA	Course of Action
COLL	Collection
COLS-NA	Columbus Network Assurance
CONOPS	Concept of Operations
CONUS	Continental United States
COOP	Continuity of Operations
COTR	Contracting Officer's Technical Representative
COTS	Commercial off-the-Shelf
CP	Content Provider
CPU	Central Processing Unit
CTNOSC	CONUS Theater NetOps and Security Center
CTO	Chief Technology Officer
CYBERCON	Cyber Operations Condition
DAA	Designated Approving Authority
DB	Development and Business Center
DBC	Defense Business Council
DBSMC	Defense Business Systems Management Committee
DCAS	Defense Cash Accountability System

Acronym	Definition
DCC	DISA Command Center
DECC	Defense Enterprise Computing Center
DFAS	Defense Finance and Accounting Service
DISB	Disbursement
DISR	DoD Information Technology Standards Registry
DRS	Dynamic Resource Scheduling
DIACAP	DoD Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DITPR	DoD Information Technology Portfolio Repository
DMZ	Demilitarized Zone
DNC	DISA NetOps Center
DNS	Domain Name Server
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoDIN	Department of Defense Information Network
DPAS	Defense Property Accountability System
DRA	Documented Risk Acceptance
DSD	Data System Designator
DVR	Digital Video Recorder
EBN	Enterprise Backup Network
ECA	Enclave Connection Authority
ECA	External Certificate Authority
ELO	External Liaison Officer
eMASS	Enterprise Mission Assurance Support Service
EOC	Enterprise Operations Center
EOL	End-of-Life
ePO	Enterprise Policy Orchestrator
EIS	Enterprise Information Services
EIS-NA	Enterprise Information Services – Network Assurance
ETA	Education, Training, and Awareness
EULA	End User License Agreement
EVS	External Vulnerability Scan
FAQ	Frequently Asked Question

Acronym	Definition
FC	Fibre Channel
FISMA	Federal Information Security Management Act
FMLO	Financial Management Liaison Office
FOC	Full Operational Capability
FQDN	Fully Qualified Domain Name
FRG	First Responders Guide
FSO	Field Security Operations
FY	Fiscal Year
GAO	General Accounting Office
GIAP	GIG Information Assurance Portfolio
GNSC	Global NetOps Support Center
GOTS	Government off-the-Shelf
HA	High Availability
HBA	Host Bus Adapter
HBSS	Host Based Security System
HIPAA	Health Insurance Portability and Accountability Act
HP	Hewlett-Packard
IA	Information Assurance
IAC	Invoice Account Code
IAM	Information Assurance Manager
IASE	Information Assurance Support Environment
IATT	Interim Authority To Test
IAVA	Information Assurance Vulnerability Alert
IAVM	Information Assurance Vulnerability Management
IAW	In Accordance With
IBE	Initial Business Estimate
IDPS	Intrusion Detection and Prevention Systems
IDS	Intrusion Detection System
IECA	Interim Enclave Connection Authority
IFAS	Industrial Fund Accounting System
IM	Instant Messaging
INFOCON	Information Operations Condition
I/O	Input/Output
IOC	Initial Operational Capability

Acronym	Definition
IOE	Initial Operating Environment
IP	Internet Protocol
IPC	Interim Production Connection
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IPAC	Intra-Governmental Payment and Collection System
IRB	Investment Review Board
IRRT	Incident Readiness Response Team
IS	Implementation and Sustainment Center
ISSM	Information System Security Manager
IT	Information Technology
I&W	Indications and Warning
J2	Joint Chiefs Intelligence
J3	Joint Chiefs Operations
JCD	Joint CERT Database
JTA	Joint Technical Architectural
JTF-GNO	Joint Task Force – Global Network Operations
KO	Contracting Officer
LE	Letter Estimate
LECA	Local External Certification Authority
LIECA	Local Interim External Certification Authority
MA	Malware Analysis
MAC	Mission Assurance Category
MNP	Malware Notification Protection
MIAG	Mandatory IA Guidance
MPI	Mission Partner Integration
MIPR	Military Interdepartmental Purchase Request
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NAS	Network Attached Storage
NAT	Network Address Translation
NAWO	Network Assurance Watch Office
NDAA	National Defense Authorization Act
NDCI	Negligent Discharge of Classified Information

Acronym	Definition
NetOps	Network Operations
NIPRNet	Non-secure Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSM	Network Security Monitoring
OE	Operating Environment
OMB	Office of Management and Budget
OOB	Out-of-Band
OPS	Operations
OS	Operating System
OSD	Office of the Secretary of Defense
OUSD	Office of the Under Secretary of Defense
PDC	Primary Domain Controller
PE	Planning Estimate
Pen Test	Penetration Test
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PM	Program Manager
PMO	Program Management Office
POA&M	Plan of Action and Milestones
POC	Point of Contact
POP	Period of Performance
PPS	Ports, Protocols, and Services
PPSM	Ports, Protocols, and Services Management
PR/SM	Processor Resource/System Manager
RACE	Rapid Access Computing Environment
RE	Reverse Engineering
RISC	Reduced Instruction Set Computing
RMF	Risk Management Framework
RTO	Red Team Operation
SA	System Administrator
SAN	Storage Area Network
SEA	Server Enterprise Architecture
SIP	Service Improvement Plan
SIPRNet	Secure Internet Protocol Router Network

Acronym	Definition
SLA	Service Level Agreement
SMC	Systems Management Center
SME	Subject Matter Expert
SSL	Secure Socket Layer
SRF	Service Request Form
SRG	Security Requirements Guide
StEA	Storage Enterprise Architecture
STIG	Security Technical Implementation Guide
STE	Secure Telephone Equipment
ST&E	Security Test and Evaluation
T&C	Terms and Conditions
T&D	Test and Development
TAS	Treasury Account Symbol
TASKORD	Task Order
TNC	Theater NetOps Center
TPN	Trading Partner Number
TRO	Targeted Response Option
TTPs	Tactics, Techniques and Procedures
UCAO	Unclassified Connection Approval Office
USC	United States Code
USCC/USCYBERCOM	United States Cyber Command
USSTRATCOM	United States Strategic Command
VA	Vulnerability Assessment
VAA	Vulnerability Analysis and Assessment
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
WAN	Wide Area Network
WCF	Working Capital Funds
WVS	Web Vulnerability Scan
z/Linux	Linux on System z

Appendix E – Glossary

Term	Description
Accreditation	Formal declaration by a DAA/AO that an information system is given approval to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. (DoDI 8510.01)
Authorization to Operate (ATO)	Authorization granted by a DAA/AO for a DoD information system to process, store, or transmit information. An ATO indicates a DoD information system has adequately implemented all assigned IA controls to the point where residual risk is acceptable to the DAA/AO. ATOs may be issued for up to 3 years. (DoDI 8510.01)
Bill	A Standard Form 1080, issued by DFAS, which constitutes an official request to pay for services delivered. Bills present only summary data on charges to the partner. Detailed charge information supporting the bill can be found on the invoice available via CIS.
Business Continuity Plan (BCP)	Advance arrangements and procedures which enable an organization to respond to an event in such a manner that the critical business functions continue with minimal interruption or essential change.
Certification	Comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements. (DoDI 8510.01)
Charges	Amount the partner is required to pay for the services provided.
Confidentiality Level (CL)	Determined by whether the system processes classified, sensitive, or public information.
Customer Account Representative (CAR)	A representative of DISA who serves as the primary POC to the partner for DISA services. The CAR is responsible for ensuring the partner is satisfied with DISA services.
Designated Approving Authority(DAA) / Authorizing Official (AO)	Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. (DoD 8510.01)
DoD Components	The United States Deputy Secretary of Defense (and all sub-components), the Military Departments, and the Joint Chiefs of Staff
Domain Name Service (DNS)	An Internet service that translates domain names into IP addresses.

Term	Description
Downtime	Time when the system or network is not available to the user. The downtime may be scheduled, as for routine maintenance, or unscheduled.
Enclave Connection Authority (ECA)	Authority to connect a device/asset to the DISA networks granted by process compliance for interim connections and granted by the managing DISA designated official for full production activity.
Exceptions to Normal Processing	Temporary requirements that cannot be accommodated within agreed-to levels of services or customary procedures.
External Certificate Authority (ECA) Program	The DoD has established the ECA program to support the issuance of DoD-approved certificates to industry partners and other external entities and organizations. The ECA program is designed to provide the mechanism for these entities to securely communicate with the DoD and authenticate to DoD information systems. The DoD Public Key Infrastructure (PKI) PMO has designated the ECA External Liaison Officer (ELO) as the single POC to receive and coordinate all communications between the ECA community, DoD programs, and the DoD PKI PMO.
Full Operational Capability (FOC)	A system is declared FOC when it has been migrated into DISA service and has executed its function for the agreed-to period (30 days after IOC declaration) without critical or high incidents, and it has completed all other defined exit criteria.
In-Cycle Changes	Refers to permanent changes to workload estimates or technical requirements occurring during the term of the SLA.
Initial Operational Capability (IOC)	A system reaches IOC when the application has been loaded, tested, and opened to the user base for production.
Initial Operating Environment (IOE)	A system reaches IOE when accepted proposals/LEs have IT assets that have progressed successfully through implementation and have been turned over to the partner to load their application(s) and data.
Interim Enclave Connection Authority (IECA)	Connection authority granted for device interim connections to the DISA Out-of-Band Network (OOB) and EBN in order to complete compliance.
Interim Production Connection (IPC)	Certain systems require connection to the production network for OS and software installation. This connectivity is limited to the site and traffic will be blocked to wide area networks (WANs). Site ISSM will acknowledge requirement for IPC and that status will be reflected in the documentation provided for Local Interim External Certification Authority (LIECA). Central Communications Center (CCC) will review the documented IPC requirement prior to activating production ports under LIECA connection status. Documentation for this process includes a justification/explanation of the requirement and validation through the site ISSM.

Term	Description
Invoice	A detailed listing of the type and quantity of services used by the partner for the period of time indicated, and the related charge to the partner for those services.
Letter Estimate (LE)	An LE is a formal document submitted to the partner as a result of a request for new, or changes to existing, workload. The LE restates the partner's expectations/mission, requirements, assumptions, and the recommended technical solution. It also includes the estimated cost for implementation and sustainment of the new or changed workload. LEs establish the basis for, or changes to, the SLA.
Local External Certification Authority (LECA)	LECA is the final network connection approval required before a device can be connected to the DISA production network accessible to WANs. Mandatory IA Guidance (MIAG) criteria compliance has been demonstrated to the approval authority and connection approval has been granted. Local Authority to Connect (ATC) is differentiated from ATC as is described in DISA Connection Approval Process (CAP) documents, and in this document only applies to DISA internal processes. The MIAG contains the complete list of documentation required to be submitted to the approving authority for approval.
Local Interim External Certification Authority (LIECA)	LIECA is the connection status assumed by a device as it is being prepared for production network connection. MIAG criteria are applied to the device as is applicable for 'interim' connection to the OOB, EBN, and in special cases, limited production network access. LIECA is differentiated from IECA as is described in DISA CAP documents, and in this document only applies to DISA internal processes. For this process, the required documentation is an email that contains the following information: • device name • IP address of the new device • hosting site • managing site • connection type requested ISSM notification should also be included in the process.
Modification/Amendment	A modification or amendment refers to changes in word or form of the existing language contained in the SLA to accommodate changed requirements. This includes changes to workload requirements. Modification of, or amendments to, the SLA may be requested by either party and must be in writing. These changes require the approval of both parties and should have sufficient lead-time to permit appropriate resource adjustments to be made. Negotiations shall be between the DISA and partner POCs identified in the SLA. Unless amended or cancelled, the terms and provisions of the SLA shall remain in effect. *NOTE: For small modifications such as POC updates, formal approval is not necessary but all parties shall be informed of the change.*

Term	Description
Operating Environment (OE)	The OS on the server, i.e. Windows, Linux or UNIX
Partner	The Service or Agency for which DISA provides services.
Planning Estimate (PE)	An estimated project cost for sustainment of services provided to the partner each FY (Oct – Sept).
Renewal	The partner and DISA shall review the SLA annually, and as required, to determine if modifications or amendments are needed to reflect the partner's support requirements for the next FY, and to accurately reflect any changes to operational policy. The PEs shall be renewed no less than annually and shall be reconciled to the SLA as part of an annual SLA review. Negotiations shall be between the DISA and partner POCs identified in the SLA. Unless amended or cancelled, the terms and provisions of the SLA shall remain in effect indefinitely.
Service Catalog	Provides descriptions of each service DISA offers, as well as services being developed in the pipeline.
Service Level Agreement (SLA)	A formal agreement documenting the services that DISA provides to the DoD Service and Agency partner.
The Agreement	The provisions set forth in the SLA, PE, Service Catalog, and T&C, together with all modifications and amendments that constitute the entire agreement between DISA and the partner.

Appendix F – References

Both parties shall comply with directives, instructions, regulations, and guidance issued by the DoD including, but not limited to:

1) CJCS Instruction 6510.01F, Information Assurance and Computer Network Defense, October 2013
http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf

2) DISA Instruction 210-225-2, Privacy Program, 6/10/2013
http://www.disa.mil/About/DISA-Issuances/~/media/Files/DISA/About/Publication/Instruction/di2102252.pdf

3) DISA Instruction 630-225-8, Freedom of Information Act (FOIA) Program for DISA, 2/5/2014
http://www.disa.mil/About/DISA-Issuances/~/media/Files/DISA/About/Publication/Instruction/di6302258.pdf

4) DoD Directive (DoDD) 5105.19, Defense Information Systems Agency (DISA), July 2006
http://www.dtic.mil/whs/directives/corres/pdf/510519p.pdf

5) DoDD 8500.01E, Information Assurance, April 2007
http://dodcio.defense.gov/Portals/0/Documents/DIEA/850001p.pdf

6) DoD Financial Management Regulation 7000.14-R, January 2012
http://comptroller.defense.gov/fmr

7) DoD Financial Management Regulation 7000.14-R, Volume 11B, Reimbursable Operations, Policy and Procedures – Working Capital Funds (WCF), December 2010
http://comptroller.defense.gov/fmr

8) DoDI 5200.01, DoD Information Security Program and Protection of Sensitive Compartmented Information, June 2011
http://www.dtic.mil/whs/directives/corres/pdf/520001p.pdf

9) DoDI 8500.01, Cybersecurity, March 2014
http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf

10) DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), March 2014 (formerly DoD Information Assurance Certification and Accreditation Process [DIACAP], November 2007)
http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf

11) DoDI 8551.01, Ports, Protocols, and Services Management (PPSM), May 2014
http://www.dtic.mil/whs/directives/corres/pdf/855101p.pdf

12) DoDI O-8530.2, Support to Computer Network Defense, March 2001
http://www.dtic.mil/whs/directives/corres/pdf/O85302p_placeholder.pdf

13) DoD Internet-NIPRNet DMZ Technology STIG Overview (NIPRNet DoD DMZ Policy Requirements), Version 3, Release 1, July 2015
https://disa.deps.mil/ext/cop/iase/stigs/Documents/fouo_dod_internet-niprnet_dmz_technology_v3r1_stig.zip

14) DoD JTA Volume II, Version 6.0, October 2003
www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA443892

15) DoD Manual (DoDM) 5200.01, Volume 3, DoD Information Security Program: Protection of Classified Information, February 2012
http://www.dtic.mil/whs/directives/corres/pdf/520001_vol3.pdf

16) DoD Memorandum, Interim Guidance on Networthiness of Information Technology (IT) Connected to DoD Networks, November 2011
http://www.disa.mil/network-services/~/media/Files/DISA/Services/UCCO/DoD_Networthiness_Memorandum.pdf

17) Federal Information Security Management Act (FISMA)
http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

18) GAO Information Technology – A Framework for Assessing and Improving Enterprise Architecture Management, Version 1.1, GAO-03-584G, April 2003
http://www.gao.gov/new.items/d03584g.pdf

19) National Defense Authorization Act (NDAA) for FY 2014, December 2013
http://www.gpo.gov/fdsys/pkg/CPRT-113HPRT86280/pdf/CPRT-113HPRT86280.pdf

20) NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

21) Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, February 1996
http://www.whitehouse.gov/omb/circulars_a130

22) Public Law 107-347, E-Government Act of 2002, December 2002
http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf

23) Security Technical Implementation Guides (STIGs)
http://iase.disa.mil/stigs/Pages/index.aspx

24) USC, Title 10, Subtitle A, Part I, Chapter 7, Section 186, Defense Business System Management Committee, January 2007
http://www.gpo.gov/fdsys/granule/USCODE-2006-title10/USCODE-2006-title10-subtitleA-partI-chap7-sec186/content-detail.html

25) USC, Title 10, Subtitle A, Part IV, Chapter 131, Section 2208, Working-Capital Funds, January 2012
http://www.gpo.gov/fdsys/granule/USCODE-2011-title10/USCODE-2011-title10-subtitleA-partIV-chap131-sec2208/content-detail.html

26) USC, Title 10, Subtitle A, Part IV, Chapter 131, Section 2222, Defense Business Systems: Architecture, Accountability, and Modernization, January 2012
http://www.gpo.gov/fdsys/granule/USCODE-2011-title10/USCODE-2011-title10-subtitleA-partIV-chap131-sec2222/content-detail.html

27) USCC TASKORD 13-0613, Directive to Scan Public DoD Websites for Vulnerabilities, June 2013
https://www.cybercom.smil.mil (*NOTE: This is a SIPRNet link; orders on bottom right)*

Document Source

1) All DISA Instructions
   http://www.disa.mil/About/DISA-Issuances/Instructions
2) All DoD Issuances
   http://www.dtic.mil/whs/directives/
3) All OMB Circulars
   https://www.whitehouse.gov/omb/circulars_default#numerical

Appendix G – Performance Standards

These performance standards are available to all DISA partners.

DISA shall make a good faith effort to meet or exceed the following operational objectives. Circumstances beyond DISA control (i.e. commercial power outages, natural disasters, inefficient application software releases, partners' local communications problems, etc.) are excluded. DISA will take prompt corrective action when these objectives are not being met.

Service	Service Objective	Service Description
Interactive Availability	98.5 percent availability	Portion of network/system controlled by DISA available to the partner during the interactive window.
Batch Throughput (mainframe)	95 percent or better completion rate and delivery	Completion rate and delivery by specified time during the batch window specified in the SLA. Partner initiated batch-processing outside the batch window will be processed as resources permit.
Job Failure Notification	Within 30 minutes	During normal working hours. Notification will be made after duty hours as requested by the partner.
Data Retrieval Services	15 Minutes 4 Hours 36 Hours	Tape, on-site (mount) Tape, off-site (local) Tape, off-site (backup site)
Server Capacity Utilization Reports	As requested	Provides previous month's capacity utilization reports for 1) most DISA-provided server hardware, and 2) partner-provided server hardware for which the partner is paying Hardware Services.
Centralized Invoice System (CIS)	Bi-weekly	Billing amounts charged to Military Interdepartmental Purchase Requests (MIPRs) at the service level.

Appendix H – Global Content Delivery Service Performance Standards/Responsibilities

The following performance standards and responsibilities pertain only to partners utilizing the Global Content Delivery Service (GCDS).

DISA:

1. Will provide immediate failover to a redundant GCDS node for disaster recovery.
2. Will provide GISMC (Tier 0) response to the partner issue within two hours of receipt.
3. Will provide triaged (Tier 1 or 2) response of the partner issue within 24 hours.
4. Will provide a quarterly evaluation of partner usage and performance.
5. Will notify the partner if the portal requires maintenance 72 hours prior to the maintenance event.
6. Will provide log delivery and accessibility for 30 days on GCDS (the partner must enable).
7. Is not responsible for the content, look, and feel of the website and/or the partner apology page.
8. Is not responsible for broken links on a website or failure of pages or graphics to load on the page.
9. Will monitor the integrated URLs accessibility, performance, and status 24x7/365 on both the NIPRNet and SIPRNet.
10. Will notify the partner immediately if there is a technical issue related to their application.
11. Will notify NetStorage subscribers if their NetStorage allocation is reaching capacity.
12. Will decommission an integrated URL 30 days following a partner's decommission action. Will not refund integration costs if the URL has gone live on GCDS.
13. Will provide streaming service over the NIPRNet or SIPRNet only to the partners at no charge.
14. Will assist the partner with the setup and configuration of the encoder for the streaming event.
15. Will assist the partner with a test and rehearsal prior to the event.
16. Will schedule support for the partner's streaming efforts via the respective DISA Mission Partner Engagement Executive Team.
17. Will provide the partner with documentation to set up the streaming service.
18. Will provide the configured video stream to a global audience on the NIPRNet or SIPRNet.
19. Will provide the partner a unique URL for dissemination to the target audience.

20. Upon request, can enable digital video recorder (DVR) capabilities for the live broadcast for 48 hours to support different time zones (Should the partner wish to retain the broadcast for longer than 48 hours, integration into GCDS NetStorage will be required).
21. Is not responsible for the hardware or software based media encoders used for the streaming event.
22. Is not responsible for the performance of the software-based media encoder on the computer (as a general rule, the more powerful, the better).
23. Is not responsible for troubleshooting of the network or firewall configurations at the partner's site.
24. Will make quarterly recommendations to the partner at no cost to enhance the performance of the application. The partner is under no obligation to accept these recommendations.

GCDS:

1. Will ensure the partner's URLs are available to their end users 99.9% of the time. The variable in this assessment is if the origin server is disconnected or no-longer operational. In this instance, DISA will ensure an apology page created by the partner is displayed until the origin server is re-connected or is operational again.
2. Will ensure the partner's performance metric interface, the GCDS Portal, is available to the partner 95% of the time.
3. Will provide updates to the GCDS partners via the GCDS website at http://www.disa.mil/Services/Enterprise-Services/Infrastructure/GCDS.
4. Will not decommission a URL without the partner's written consent.
5. Will not troubleshoot an application if the triage does not indicate it is a GCDS problem.
6. Will not continue integration if all 125 hours per URL are used up during the integration process.
7. Will not re-integrate a URL if the partner has decommissioned the URL from GCDS and the URL was decommissioned from GCDS.

DISA Partner:

1. Will notify the appropriate DISA Mission Partner Engagement Team in writing of their intent to decommission two weeks prior to decommission.
8. Will enable log storage on GCDS through the GCDS portal (part of the integration process).
9. Has the ability to store their logs in GCDS NetStorage indefinitely. Should this occur the partner is responsible for overwriting their logs and the specified retention or cut-off point.
10. Has the flexibility to purge an event or the entire content. If the file is purged by accident, the partner must notify GCDS via the GISMC (Email: disa.columbus.esd.mbx.gcds-columbus@mail.mil) to attempt to recover the file.
11. Understands that the data is unavailable to the end users until the propagation from the origin server is completed across the GCDS network if their entire content is purged

intentionally or accidentally. Must provide written consent to GCDS should they wish to decommission a URL.

12. Has the flexibility to decommission a URL. If this occurs, the partner understands that the URL will be decommissioned from GCDS 30 calendar days from decommission. Once the URL is decommissioned, integration back into GCDS is considered a new integration costing $40K per URL (no-recurring cost). It is strongly suggested the GCDS PMO is notified at disa.meade.esd.list.gcds@mail.mil prior to taking such action.
13. Will inform the GCDS PMO anytime a POC responsible for the management of the integrated application changes.
14. Is responsible for maintaining the allocation if the partner utilizes GCDS NetStorage.
15. Is responsible for ensuring the IA accreditation of the application is maintained. If the accreditation expires, the partner must notify the GCDS PMO immediately to suspend content delivery until the application is re-accredited.
16. Understands if their URL(s) transitioned to GCDS from DISA NCES in FY10, their content delivery continued without interruption. There was no cost associated with this transition.
17. Understands if they were brought onto GCDS with an LE, the recurring billing for GCDS stopped on September 30, 2011 due to the GCDS transition to the DISN Subscription Service (DSS).
18. Is responsible for the procurement of the broadcast media (camera, hardware or software-based encoder, production equipment).
19. Is responsible for the opening of the required ports on the local firewall to enable the streaming.
20. If using a hardware-based encoder, is responsible for the proper IA authorization and accreditation for using the hardware-based encoder.
21. Is responsible for ensuring the selected media encoder is H.264 Industry Standard compliant.
22. Is responsible for the content and the operational security associated with the streaming event.
23. Will contact the respective DISA Engagement Executive Team initiate the request for streaming support.
24. If subscribing to NetStorage, may request an apology page that will be displayed should the origin web server be unavailable. Once the GCDS network recognizes the web server is available, the apology page will revert to the partner's site.

Appendix I – Audits and Audit Readiness for Systems Impacting Financial Statements

The Office of the Under Secretary of Defense (Comptroller) (OUSD[C]) Financial Improvement and Audit Readiness (FIAR) guidance specifies the need for an agreement that articulates the service receiver and service provider relationship and the applicable audit aspects for transactions relevant to the reporting entity financial statements. Program specific service selection and any special functions provided by DISA are documented in the SLA, its attachments, and supporting documents.

This section describes general responsibilities of DISA and DISA's partners for supporting audit readiness efforts and audits affecting DoD financial statements and service providers.

Partner Responsibilities:

1) Deliver the overall mission for their systems to all DoD military and civilian employees and administer the planning, programming, budgeting, and execution for the system-related programs; remain accountable for keeping the systems operationally effective and available for their own use and use by the DoD community.
2) Review DISA's Statement on Standards for Attestation Engagements No. 16 (SSAE 16) which provides assurances needed for auditors and system owners. Any concerns should be addressed with DISA Cyber Services.
3) Ensure that auditors and system owners rely on the SSAE 16 to the greatest extent possible.
4) Partners with financial systems hosted by DISA: Evaluate and, as appropriate, implement controls that address the "Complementary User Entity Controls (CUECs)" as identified in the most recent copy of SSAE 16 report (henceforth referenced as a Service Organization Controls 1 or "SOC1" report) provided by DISA.
5) Notify DISA of systems hosted at DISA that are relevant to financial reporting.
6) Inform DISA of audit and audit readiness activities early in the process in order to properly plan.
7) Ensure special system requirements are documented and made part of the SLA; for example, include records retention requirements.

DISA Responsibilities:

1) Prepare, evaluate, and remediate DISA processes, systems, controls, and supporting documentation to support the audit readiness and financial statement audit sustainment efforts of partners and their customers.
2) Understand and be prepared to support the audit readiness timeline of partners and their customers. (This is conditional on partners informing DISA of audit and audit readiness activities early in the process; see above.)
3) Prepare for and undergo an annual SSAE No. 16 examination for which the scope includes control objectives and control activities that are relevant to partners' and their customers' internal control over financial reporting, and that culminate with DISA's issuance of a SOC 1 report no later than August 15th of each year.

4) Provide partners a description of the information system controls that may affect aspects of their control environment that are relevant to financial reporting. Information about controls can be found in this section, the IA control links in the SLA, and DISA's Hosting services SSAE16 SOC1 report.

DISA's SSAE16 SOC1 reports can be obtained from disa.meade.se.mbx.se4-fusion-center@mail.mil.

Shared Responsibilities:

1) Maintain open communication and coordinate with each other and supporting contractors.
2) Provide additional system information within agreed upon timeframes.
3) Provide access to subject matter experts or contractors supporting those organizations within agreed upon timeframes.
4) Discover and correct audit impediments that fall within the responsible party's/parties' organizational/authoritative jurisdiction(s).
5) Establish a common, detailed understanding of the scope, roles, responsibilities, required FIAR deliverables, timeline, and method for obtaining assurance (e.g., through the completion of an SSAE No. 16 examination or directly as part of *partner's* audit readiness efforts for the applicable *partner*-managed system).

Audit Support Requests:

Audit support requests related to Hosting Services shall be submitted to DISA at the following address: disa.meade.se.mbx.se4-fusion-center@mail.mil.

Requests for evidential matter will be submitted on the DISA standard form (the standard form can be requested at the above email address). Requests will be initially evaluated and acknowledged within one (1) business day. DISA will make every effort to return evidential matter in the requested period of time. If DISA is unable to support a requested time for completion, DISA will inform the partner and provide an estimated completion date. Partners should understand that clarity and completeness of requests impacts DISA's ability to respond quickly and accurately.

DISA does not release documentation of disaster recovery plans due to the sensitivity of the information; however, plans may be reviewed remotely or on site in a live session, upon request.

Recurring periodic requests should be directed through normal customer management channels and documented as part of the SLA. Examples of this type of request are periodic lists of system users and periodic reports of system activity such as logs.